IoT risks from an insurance perspective

Cyber Working Group

April 2022

Table of Contents

Introduction

It is a step into a new dimension: with the Internet of Things (IoT), the network is extending to physical reality. Not only the devices we would normally associate with accessing the Internet, but also machines, vehicles, and plants of all kinds are now equipped with sensors and digitally record in the network.

With smart connectivity, all this combines to create a fascinating ecosystem of data. But how do companies generate added value from this apparent flood of data? There are countless exciting use cases in industry, the consumer sector, and public services. However, implementing the IoT can only succeed within the context of a concrete strategic vision.

In this paper, the main definitions, characteristics, and different types of IoT are presented alongside a brief market analysis. Specifically, the dynamics of the IoT market in geographical terms and a market forecast for the next years are described.

In addition, regulations in specific geographic areas and sectors are discussed. For example, the type of data processed and the type of device may have different regulations to consider. Specific chapters outline key risk areas, which go beyond just cybersecurity risk, but also include strategic, reputational and accumulation risks related to the connected devices.

Moreover, the last chapter of this paper confirms that the rise of the IoT presents new challenges for risk managers in how they manage and control the risk. They need to adapt their risk management approaches to understand and manage the IoT risks across the business.

Therefore, this document is not only useful for providing an overview of the IoT world from a business perspective, but it can indeed be a valuable guide for insurance risk managers. Through this paper, they can identify the main challenges they will need to face and the approaches that can be adopted to overcome future obstacles.

Finally, a brief conclusion rounds off the paper, summarising the key points of each chapter of this document.

Executive summary

The Internet of Things is a fast-growing market, as reported in this paper, both in terms of production and consumption. The IoT global market size is expected to reach USD 1,463.19 billion by 2027, having risen from a previous size of USD 250.72 billion observed in 2019. Moreover, the number of IoT devices worldwide is expected to almost triple from 8.74 billion in 2020 to more than 24.1 billion IoT devices in 2030.

Given the expected growth rates of this market, IoT will certainly represent an opportunity for different sectors, including the insurance industry, but may also entail numerous risks to be managed. With the aim to defend businesses and consumers from the risks posed by the IoT, different regulations and best practices have been issued in several countries. Indeed, there is an ongoing scramble to develop specific guidelines and standards across sectors, but in case of absence of specific instructions for the IoT, general ICT rules are still used.

Therefore, considering that IoT regulation is still in a consolidation phase, in order to take full advantage of the opportunities that IoT can offer, insurers will need to be able to manage the related risks, such as: cybersecurity, strategic, reputational and accumulation risk.

Risk managers and insurers will face new challenges in terms of risk management and risk control, and they will need to include the IoT in their risk management framework to properly handle the related risks. Risk managers and insures, whether relying on IoT to collect data for insurance purposes or extending cover to clients who are themselves device owners, must perform an appropriate due diligence on the IoT involved, in order to properly manage the operational risk.

Moreover, they will need to take care of the accumulation risks as well, by identifying the related mitigation actions that can be performed to prevent an accumulation event. In addition, risk managers and insurers need to support the development of quantification approaches to measure these risks and use them to get comfortable on accepting the accumulation risk associated with IoT.

Therefore, as reported in the paper, the advent of IoT will bring several opportunities and risks. The goal for risk managers and insurers will be to better manage the risks arising from IoT, in order to take advantage of the opportunities presented by this new trend. To achieve this goal, risk managers can use this paper as a solid guide.

1. What is IoT

1.1 History and background

The Internet of Things (IoT) comprises a wide ecosystem of interconnected services and devices, such as; smart consumer products, everyday smart home objects, cars, industrial and health components. These technologies collect, exchange and process huge amounts of data in order to analyse and dynamically adapt to a specific context. This hyper-connection between people, machines, and organisations is a prevalent trend at almost all levels of society and around the world transforming the way we live and how we do our businesses.

The IoT as a concept has not been around for very long. It was introduced in 1999 by Kevin Ashton, the Executive Director of Auto-ID Labs at Massachusetts Institute of Technology (MIT), while making a presentation for Procter & Gamble. Ashton who was working in supply chain optimisation, wanted to attract senior management's attention to a new technology called Radio Frequency Identification (RFID). Because the internet was the trend in 1999, and because it somehow made sense, he called his presentation "Internet of Things".

During his 1999 speech, Mr. Ashton stated:

> "Today computers, and, therefore, the Internet, are almost wholly dependent on human beings for information. Nearly all of the roughly 50 petabytes (a petabyte is 1,024 terabytes) of data available on the Internet were first captured and created by human beings by typing, pressing a record button, taking a digital picture or scanning a bar code. The problem is, people have limited time, attention, and accuracy, all of which means they are not very good at capturing data about things in the real world. If we had computers that knew everything there was to know about things, using data they gathered without any help from us, we would be able to track and count everything and greatly reduce waste, loss, and cost. We would know when things needed replacing, repairing, or recalling and whether they were fresh or past their best."

The roots of RFID technology can be traced back to World War II where it was used to differentiate friendly planes from enemy planes. Advances in RFID systems continued in the 1950s and 60s to identify objects remotely. Companies began commercialising anti-theft systems that are still used in packaging today. Other examples of RFID systems developed throughout the years are but not limited to: access control systems, toll payment systems, anti-theft devices for cars, livestock tracking, warehouse tracking, payment systems, and contactless smartcards. Kevin Ashton believed RFID was a prerequisite for the IoT. He concluded if all devices were "tagged", computers could manage, track, and inventory them. Tagging of things is achieved through various technologies such as digital watermarking, barcodes, and QR codes. Inventory control is one of the first main use-cases of the IoT and essentially changed the way how RFID was used. The technology had been turned into a networking technology by linking objects to the internet through tag's creating an IoT.

During the last decade, the IoT usage is maturing in both corporate and consumer environments like consumer wearables, smart home equipment, industrial control systems, smart cities, and airports, cars, health devices etc. Current IoT applications are explored within the next chapters of the document.

According to a recent report by Kaspersky the adoption of the IoT is steadily growing in all industries: 61% of enterprises already use IoT applications. Use is expected to increase year on year as sensors evolve and become smaller, harness greater computing power, leverage greater connectivity capability (5G) and apply artificial intelligence (AI) techniques to data. As we will see in the following section "Market Analysis", the number of IoT devices worldwide is forecast to almost triple from 8.74 billion in 2020 to more than 24.1 billion IoT devices in 2030. In other words, there will be four IoT devices per human being.

Figure 1: The Internet of Things

Although IoT is a mega trend at almost all levels of society, a unique definition of IoT is not available. IoT solutions consists of four elements such as **Devices** (Sensors and actuators), **Communication networks**, **Analytics** and the **Application layer**. Its applications can be broadly classified into five areas (industrial, commercial, healthcare, transportation, and consumer).

1.2 Definitions and characteristics of IoT

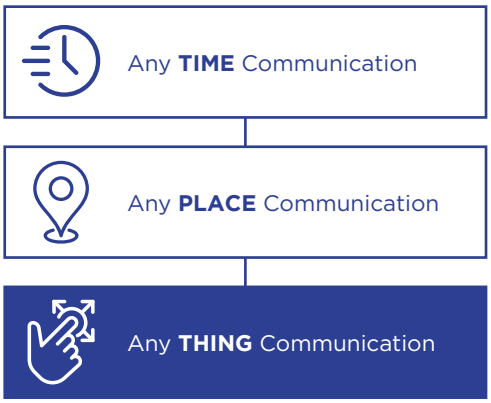
The IoT has many definitions and there is no universally accepted definition yet, but definitions typically have common elements like sensors, network connectivity, physical and virtual things, and intelligent decision making. Some examples of these definitions are:

- European Agency for Cyber Security (ENISA):
  "a cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision making."
- The Institute of Electrical and Electronics Engineers (IEEE):
  "A network of items—each embedded with sensors—which are connected to the Internet."
- The International Telecommunications Union (ITU):
  "A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies (ICT)."
- The Internet Engineering Task Force (IETF):
  "The network of physical objects or "things" embedded with electronics, software, sensors, actuators, and connectivity to enable objects to exchange data with the manufacturer, operator, and/or other connected devices."
- The US National Institute of Standards and Technology (NIST):
  "User or industrial devices that are connected to the internet. IoT devices include sensors, controllers, and household appliances." And "The network of devices that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information."
- McKinsey:
  "Sensors and actuators connected by networks to computing systems. These systems can monitor or manage the health and actions of connected objects and machines. Connected sensors can also monitor the natural world, people, and animals."
- Oracle:
  "The Internet of Things (IoT) describes the network of physical objects — "things"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet."
- The IERC (IoT European Research Cluster - European Research Cluster on the Internet of Things):
  "A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network."

1.2.1 Characteristics

The International Telecommunications Union explains in their overview of the IoT that the concept adds the dimension "Any THING communication" to the Information and Communication Technologies (ICTs) which already provided "any TIME" and "any PLACE" communication.

Figure 2: Any THING communication



Regarding the IoT, things are considered objects of the physical world (physical things) or of the information world (virtual world) that are capable of being identified and integrated into communication networks. Things have associated information, which can be static and dynamic.

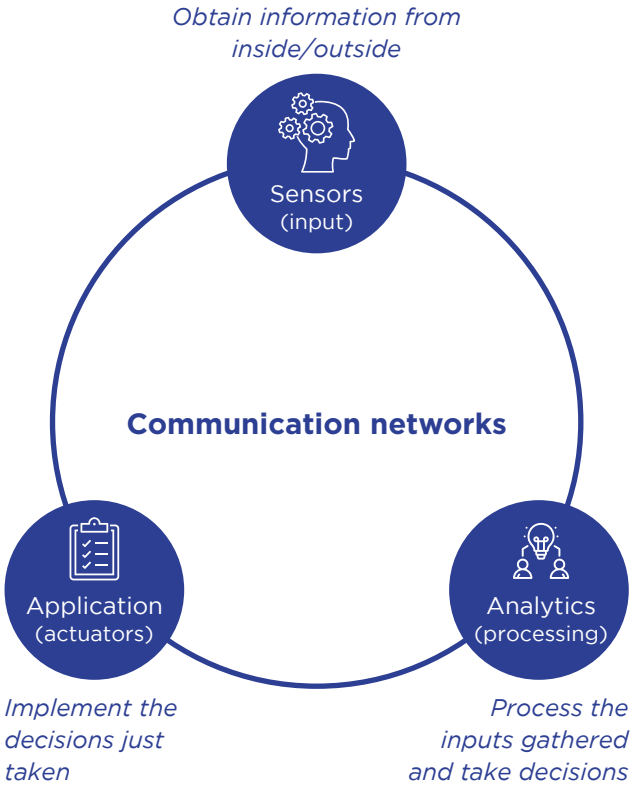
Physical things exist in the physical world and are capable of being sensed, actuated, and connected. Examples of physical things include the surrounding environment, industrial robots, goods, and electrical equipment.

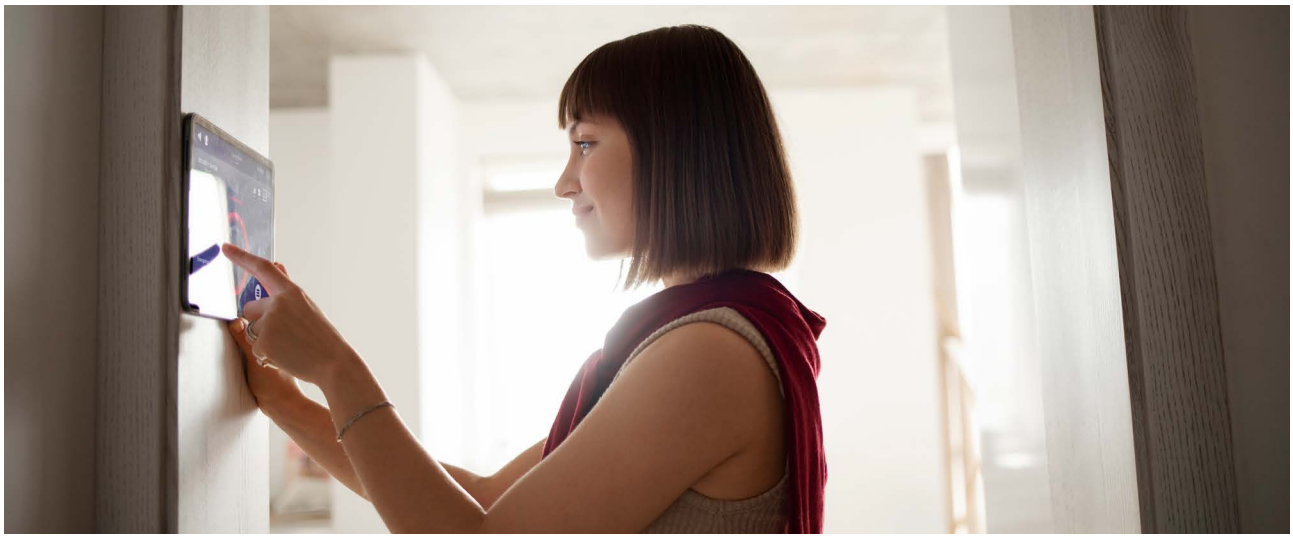
Virtual things exist in the information world and are capable of being stored, processed, and accessed. Examples of virtual things include multimedia content and application software.

1.3 IoT Architecture

In general, an IoT solution consists of four elements. **Devices** (sensors and actuators), **Communication networks**, **Analytics** and the **Application layer** (actuators). Together these components form the IoT ecosystem and allow information to be used for intelligent decision-making and take smarter actions that would otherwise be impossible in the traditional, disconnected, physical world.

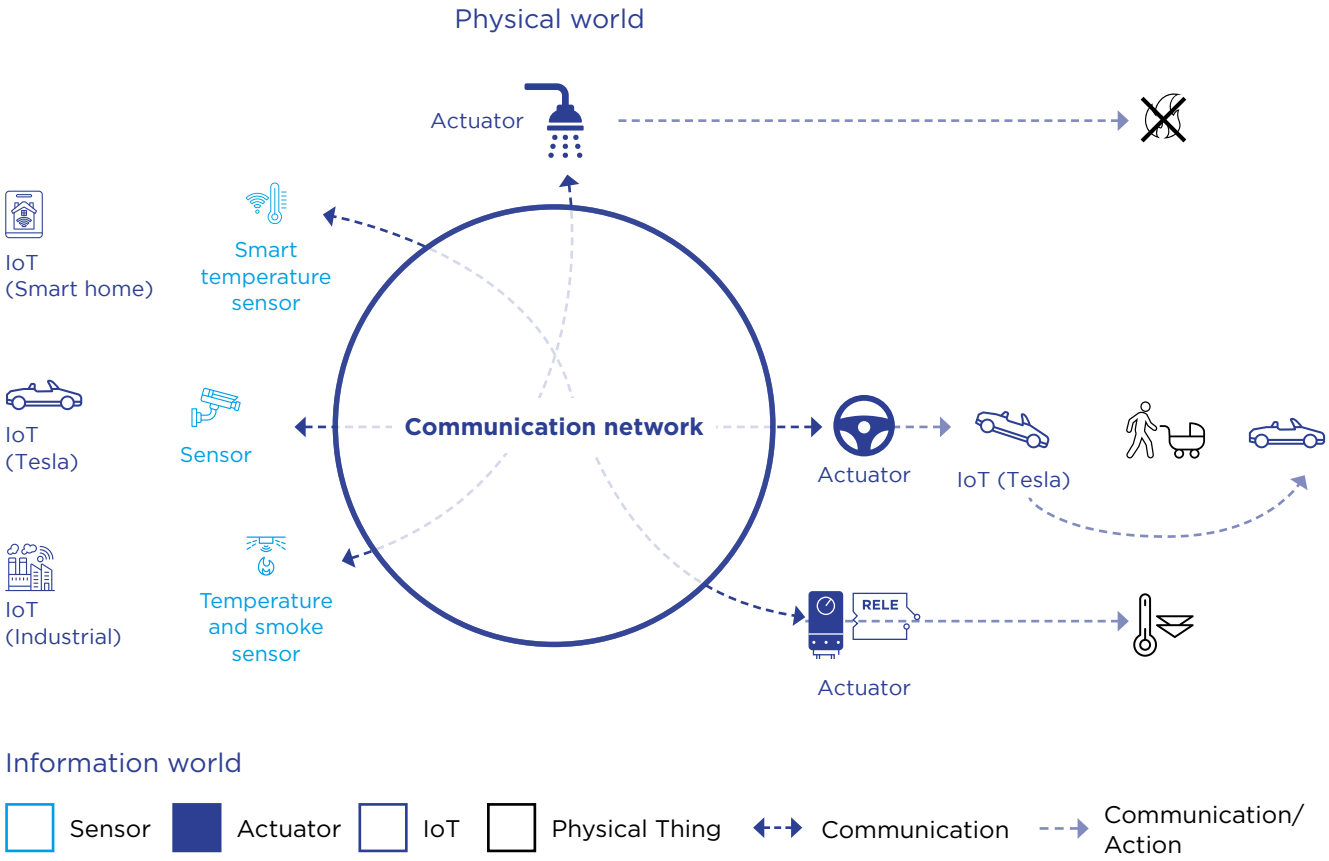
Figure 3: Abstract of ecosystem architecture





A more technical overview of the IoT architecture is represented in figure 4.

Figure 4: IoT architecture



A physical thing may be represented in the information world via one or more virtual things (mapping), but a virtual thing can also exist without any associated physical thing.

A device, or thing, is a piece of equipment with the capabilities of communication and optional capabilities of sensing, actuation, data capture, data storage, and data processing. Devices collect various kinds of information and provide it to the information and communication networks for further processing. Some devices also execute operations based on information received from the information and communication networks. More specifically, the main characteristics of an IoT device could be the following ones:

- **Dynamic and Self-Adapting:** given a new context, connected devices should adapt, change their actions, and modify their decisions.
- **Self-Configuring:** devices can configure themselves, setup a network, make a connection, and fetch the latest software updates, all with minimal or no user intervention.
- **Interoperable communication:** the IoT should support communication between a variety of brands of devices in order to create a network with greater connectivity and improved efficiency.

Therefore, devices are able to communicate with other devices: they communicate through the communication network via a gateway (case a), through the communication network without a gateway (case b) or directly, i.e., without using the communication network (case c). Also, combinations of cases a and c, and cases b and c are possible; for example, devices can communicate with other devices using direct communication through a local network (i.e., a network providing local connectivity between devices and between devices and a gateway, such as an ad-hoc network) (case c), and then communication through the communication network via a local network gateway (case a).

The communication networks transfer data captured by devices to applications and other devices as well as instructions from applications to devices. The communication networks provide capabilities for reliable and efficient data transfer. The IoT network infrastructure can be wireless or wired based via existing networks, such as TCP/IP-based networks, and/or 4G and more recently, 5G.

The IoT applications include various kinds of application types, e.g., "intelligent transportation systems", "smart grid", "e-health" or "smart home". The applications may be based on proprietary application platforms but can also be built upon common service/application support platform(s), thus providing generic enabling capabilities, such as authentication, device management, charging, and accounting. Further IoT applications are explored within the next section of the document "Type of IoT".

1.4 Type of IoT

Although many different classifications are possible, adopting an insurers' perspective, use of the IoT technology can be broadly classified into five areas: industrial, commercial, healthcare, transportation, and consumer.

1.4.1 Industrial IoT

Industrial IoT, also known as IIoT, targets existing automated industrial systems seeking improvements in efficiency, automation and connectedness. The positive impact that IoT solutions have brought about is so important that many talk about a major driver for the Fourth Industrial Revolution. Industrial IoT solutions aim to optimise current processes by implementing new features such as remote control or process monitoring, as well as the use of sensors directly placed on machines to perform predictive and preventive maintenance. It is worth mentioning some of the IoT categories that exhibit enormous potential even on a standalone basis:

- **Manufacturing:** IoT solutions can be applied to various manufacturing devices to add detection, identification, processing, communication, actuation and networking capabilities. The benefits can be seen for instance in equipment management, resource management/control, plant optimisation, and health and safety management. Workers' safety is a relevant use case: wearables used by workers provide a real-time feedback to the worker, as the wearable sets off an automatic vibration in case of exposure to a risky situation or environment. Devices are also used to generate detailed pictures of workplace risks, thus allowing the employer to strategically coach, correct, and implement actionable safety-forward interventions. A recent use case relates to mitigating COVID-19 risk by providing real-time physical distancing alerts, interaction frequency/duration data, and accurate contact tracing reports.
- **Agriculture:** IoT solutions are used for predictive maintenance and equipment care as well as continuous monitoring of the cultivation environment and product yield; watering management and optimisation is also widespread.
- **Utilities:** remotely managed meters, also known as smart meters, allow users to optimise consumption. Another use case is leak and freeze detection with real-time alerts.
- **Smart Cities and Infrastructure:** smart cities can take advantage of real-time analysis and automated actions, for example in the areas of traffic control, energy use, and motorway maintenance.

1.4.2 Commercial IoT

The Commercial IoT targets our daily environment outside of the home. There is a set of applications that can be deployed in places such as commercial office buildings, supermarkets, stores, hotels, healthcare facilities, or entertainment venues. Applications are many: monitoring environmental conditions, performing access management, connected lighting, resource monitoring, and much more. These applications provide, for example, better guest experiences through more efficient monitoring in smart buildings and smart offices and can mitigate their business risks through IoT-based services, such as detecting when fridge room doors are open to avoid food spoilage.

1.4.3 Healthcare IoT

IoT devices can be used to enable remote health monitoring and emergency notification systems that enable early diagnosis, care optimisation, and therapy adherence. Use cases in health monitoring can range from blood pressure and heart rate measurement to advanced applications with specialised implants like pacemakers. The use of sensors and mobile devices provides real-time 24/7 information and enables symptoms and disease monitoring. Patients can share their data with doctors, nurses, and family members, as well as with machines that provide automatic feedback through algorithms.

1.4.4 Transportation IoT

A dynamic interaction among the components of transport systems enables inter and intra-vehicular communication, intelligent traffic control, intelligent parking, toll collection systems, logistics, and fleet management, vehicle control, preventive safety, and assistance. Use cases include tracking inventory data and just-in-time production. In fleet management, it becomes easier to perform routing, to track vehicles, and to handle maintenance schedules. Telematics technology also improves drivers' safety through driving behaviour alerts, collision prevention, and driver distraction/fatigue detection.

1.4.5 Consumer IoT

This type of IoT includes devices that are already widely disseminated throughout our lives such as smart TVs, smart speakers, toys, wearables, and smart appliances. Health and fitness monitoring devices, like smart watches, can provide customised nutrition, sleep and physical activity advice based on customer's profiles and activities. In a smart home, users can minimise the cost of water and electricity. Consumer use cases also include services already mentioned in Commercial IoT like smart, cheaper heating/cooling and water leakage detection.

1.4.6 Benefits

The greatest benefits to consumers, the environment, and enterprises by all types of IoT is due to real-time data collection and processing. Below is a non-exhaustive list of IoT advantages:

- Work and home safety enhancement
- Better health, disease prevention and longer life expectancy
- Improved quality of life
- Better and more personalised customer experience
- Reduced resources consumption
- Prevention of breakdowns and timely detection of adverse events
- Optimised business processes and automated daily activities
- Cost-savings

The availability of a huge amount of data, much of them in real time, also provides opportunities from an insurance perspective. The IoT-enabled services enhance the insurers' ability to develop new risk assessment and prevention services that, correspondingly, reduce claims. Generating value for both customers and themselves in a win-win adoption of the IoT, insurers can promote less risky behaviours as well as safer workplaces and healthier lifestyles. Furthermore, with better risk knowledge, products can be better customised and certain previously uninsurable risks can become insurable. In turn, as more accurate and timely information becomes available, IoT solutions allow the optimisation of insurance business processes such as underwriting and claims management. Further IoT use cases related to the insurance sector, are explored in the next section of this document (ref. paragraph: "2.4 Market overview for the Insurance industry").

2. Market Analysis

2.1 Market Dynamics by geography

2.1.1 IoT consumption

The number of IoT devices worldwide is expected to almost triple from 8.74 billion in 2020 to more than 24.1 billion IoT devices in 2030, or roughly four IoT devices per each human being. In 2020, China was the unquestionable leader of adoption of IoT devices, with 3.17 billion devices deployed.

As of today, the United States are the biggest IoT market in the world. However, it is expected that China's growth will enable it to take the first place on the podium by 2024. This is due to the increasing IoT spending in China (USD 300 billion). In third position, we can find Europe.

As of today, Europe is leading the transformation of cities into smart, digitalised urban environments. Both the EU and the member states have invested in developing solutions to make the cities more connected. Business Insiders reported that the European Commission has spent around USD 439.6 million in 2019 for "smart" projects. In 2021, Europe is planning to spend USD 202 billion on IoT, creating an attractive market for investors. In the consumer sector, this growth is based on the attractiveness and comfort of having a connected home.

The IoT market is a highly competitive environment due to the existence of both small, medium, and large companies trying to secure a share of the market. Innovation is key in order to stay attractive.

2.1.2 IoT production

IoT devices are essentially composed of two layers: the hardware and the software part. The former refers to all the integrated circuit (IC) chips, modules, transceivers and sensors, while the latter refers to the embedded logic in the device and supporting platforms to provide all the functionalities.

The main producers of IoT devices are operating in the Asia-Pacific region and the United States. Countries such as India (especially with the "Make in India" initiative), China and Japan, which are already key players in the IC chip manufacturing industry, are successfully attracting sizeable investments in IoT.

The United States market generated around USD 196 billion in revenue and has the highest number of key semiconductor companies (9 in the Top 15). This is followed by South Korea (USD 52 billion), Taiwan (USD 45 billion), Europe (USD 28 billion).

The IoT market is facing the following difficulties:

- High concentration of semiconductor component production in the Asia-Pacific region
- COVID-19 pandemic, and its impact on the workforce, factory schedules and supply chains
- Ukraine-Russia war, and its impact on the IC chips production
- High volatility of demand for IC chips and the limited flexibility of supply

An important characteristic of the globalised economy is the typical geographic separation of company headquarters from its production facilities and from its suppliers. The level of complexity of IoT global value chains is very high, reflecting the complexity of the products themselves. The majority of top players in the market are headquartered in the USA, where products and software are designed and developed. Yet, for the technology to be commercially viable, it needs to be produced at high enough scale and at lowest possible cost. The Asia-Pacific region stepped up to the challenge, rising to prominence as a systemic supplier of semiconductor-based products and device manufacturer for the entire globe. Nearly 50% of the semiconductors are produced in Taiwan, followed by South Korea, holding a further 18% share of the market. In the age of intensifying trade wars, this degree of dependency exposes the market to significant risks such as new regulations and tariffs.

The IoT global market size is expected to reach USD 1,463.19 billion by 2027 from the level of USD 250.72 billion observed in 2019 and the number of IoT devices worldwide is expected to almost triple from 8.74 billion in 2020 to more than 24.1 billion IoT devices in 2030.

The main risk the world is currently facing is related to the shortening of IC chips. Carmakers, who closed their plants during the COVID-19 pandemic last year and cancelled their orders of IC chips, are now competing against the consumer electronics industry. During the pandemic, customers have started to stock up on electronic devices such as gaming consoles, laptops, tablets, and other products, driving up the demand for semiconductor-based products. This combined with the fact that the sales of cars surpassed most industry executives' forecasts, despite the pandemic situation, put the supply side under enormous strain. The difficulties that were initially only reported in the automotive industry have now also spread to the consumer electronics. Apart from IoT devices, the availability of products considered essential, such as smartphones, refrigerators, and microwaves, are also affected.

In addition to the COVID-19 pandemic, the Ukraine-Russia war is contributing to worsening the IC chips shortage. Indeed, due to the escalation of the conflict in Ukraine which resulted in civilian deaths and infrastructures destruction, Ukraine's two leading suppliers of neon (Ingas and Cryoin), which produce about half the world's supply of this element and which is used for the chips production, have halted their operations. These companies are respectively located in Mariupol and Odessa, two cities heavily hit by Russian bombing. Therefore, if the war does not end quickly, in addition to incredible suffering, it will contribute to worsening the global production of chips, already scarce after the COVID-19 pandemic.

While companies around the world panic-buy IC chips to shore up stocks, manufacturers' flexibility in ramping up production capacity is very limited. Factories that produce microchips, semiconductors, and related components cost tens of billions of dollars to build, and expanding their capacity is a very complex process that can take up to a year for testing and validating of tools. In consequence, the cost of nearly all microchips has been substantially increasing, driving up the prices of final products.

Furthermore, the problems of high-tech industry go beyond the limit of semiconductors production capacity. The ability to satisfy the increasing demand for the devices and ensure IoT ecosystem's consistent growth, depended heavily on rare earth elements. The rare earth elements (REE) are a group of seventeen metallic elements, 15 from the "lanthanides series" in the periodic table, along with scandium and yttrium", essential for high-tech electronical components.

Therefore, as in the case of semiconductors, the rivalry to secure the supply of those raw materials is increasing in ferocity. China is clearly dominating this market and 80% of the rare earths imported by the United States from 2014 to 2017 have been supplied by the People's Republic of China. In 2017, China accounted for 81% of the world's rare earth production (data from the U.S. Geological Survey).

In a bid to question the Chinese supremacy, the United States is trying to rebuild the entire domestic supply chain related to these materials. Nevertheless, many activists are raising concern abouts the risks related to rare earth mining, from environmental to public health.

2.2 IoT consumption: Market Dynamics by type of IoT

2.2.1 Industrial IoT

With the biggest share of the IoT market, the global Industrial Internet of Things (IIoT) segment is valued at USD 82.4 Billion in 2020 and is anticipated to grow with a CAGR of 21.3% during the forecast period from 2020 to 2028. This tremendous growth is unquestionably driven by governments' support for the development and implementation of the Industrial IoT (IIoT).

In addition, organisations have developed a real interest in IIoT as the devices send data in real-time from various sources that are used to improve the decision-making process. A good example for that is the smart city, which can take advantage of real-time analysis and automated actions, for example in the areas of traffic control, energy use, and motorway maintenance.

2.2.2 Commercial IoT

The Commercial IoT aims to enrich our daily environment outside of the home. Key areas of implementation include Intelligent Asset Tracking, Smart Office and Buildings, Connected Lighting, Sensing & Monitoring of all types, and Location Services (i.e., providing contextual experiences to

guests in places like hotels and restaurants). The Commercial IoT solutions usually leverage a wide array of wireless communication technologies like Bluetooth, Wi-Fi, ZigBee, Sigfox, LoRa, and LTE.

2.2.3 Healthcare IoT

Hospitals are relying more than ever on new technologies. Doctors, nurses, and staff are using the IoT to make more accurate diagnosis, and to monitor patient's vital signs. A new trend has emerged that uses smart devices to monitor patients at home. During the COVID-19 pandemic, it's been demonstrated that tele-health consultations are feasible especially if the patients use IoT health sensors to share their health status with doctors. The IoT will be essential in providing better care to patients all around the world. As an example, connected robots have allowed a surgeon to perform a surgery 400km away from the patients.

2.2.4 Transportation IoT

In the transportation sector, the IoT enjoys a well-established presence. For the industry, the technology can be used to monitor cargo and freight transportation allowing for real-time location or status. The IoT can also be leveraged to enhance the offering. Car manufacturers integrate increasing numbers of smart modules to their cars to make them safer and more autonomous. Cars are now connected to the internet through the cellular networks or directly to a satellite. Besides providing GPS navigation and entertainment to the driver and passengers, connected cars' software can be updated on-the-fly, leveraging the latest security and functionality improvements. An example of this would be the Tesla Model S introduced back in 2012, which continues to be relevant thanks to the continued software support.

2.2.5 Consumer IoT

The Consumer IoT (sometimes known as the "Internet of Toys") comprises a set of connected devices, whose primary consumer is the private individual or domestic market. This type of IoT includes devices that are already playing an integral part of our daily lives such as smart TVs, smart speakers, toys, wearables and smart appliances. Typically, the device has a discrete function which is enabled or supplemented by a data-gathering capability through on-board sensors and can also be used to add functionality to common domestic items, such as refrigerators.

2.3 Market Forecast for the next years

In the last few years, we have seen the development of technologies that, when combined with the IoT, will help the latter becoming more ubiquitous. Artificial Intelligence, 5G connectivity, and Big Data are the pillars of the new wave of adoption of the IoT. According to the World Economic Forum, the combination of those technologies will help develop the IoT, in particular:

- **Consumer IoT:** people are getting more and more attracted to smart accessories and wearables such as the Fitbit. They want to gather and analyse their activity levels to build healthy habits and improve their lives. According to leading tech research firm Gartner, the global wearable device market is estimated to see more than $87 billion in revenue by 2023.
- **Industrial IoT or IIoT:** Companies will require IoT not only to perform more detailed analysis on their processes in order to improve them in terms of efficiency and revenue but also to reduce errors, incidents and maintenance time.

The IoT global market size is expected to reach USD 1,463.19 billion by 2027, from the level of USD 250.72 billion observed in 2019, while exhibiting a CAGR of 24.9% during the forecast period. In 2030, it is estimated that the three main markets will be China (26%), North America (24%), and Europe (23%).

Although, one should keep in mind that these figures could be impacted by the shortage of: IC chips; conductors; and rare materials, that we currently observe even if, as at today, a clear link between both phenomena, increase of IoT demand and production and decrease of available resource, has not been quantified.

2.4 Market overview for the Insurance industry

The global Insurance IoT market is valued at USD 16.28 Billion in 2020 and is anticipated to grow with a CAGR of 62.6% during the forecast period from 2020 to 2028. While the adoption of the IoT in the insurance industry is at an early stage of maturity, it demonstrates an enormous growth potential in the coming years.

Currently, insurers have mainly used the IoT capabilities to aid interactions with customers and to accelerate and simplify underwriting and claims processing. However, the new IoT-based services and business models are gaining traction thanks to their high attractiveness to insurers. IoT enables insurers to collect more comprehensive, reliable, and higher quality customer data they can use to assess risk, which makes it possible to offer discounts or surcharges. In the context of new business models, interconnectivity enabled by IoT could become a strategic component for insurers, especially in the following areas:

- **Commercial IoT:**
  - Mobility/connected car insurance: several easily available variables such as credit score, location, type of car, miles driven per year, age and gender have helped auto insurer to measure a driver's risk. These variables provided sufficient insight to properly rate an individual based on historical trends. Nevertheless, incorporating additional variables could allow better pricing tailored to individual customers. With data from the IoT telemetry, insurers could offer special discounts to drivers who rarely exceed the speed limit and always put on their seat belts.
  - Commercial line insurance: the commercial ecosystem that is centred on the distribution to business partners (B2B or B2B2C) and on making the most of partnerships along the value chain also often focus on data and operational excellence. IoT-enabled risk prevention may include, for example, sensors in warehouses to assess risk—and hence price—on a more granular level.
- **Industrial IoT**
  Smart housing insurance: in homeowners' insurance, in case of hidden water or gas leaks, the IoT data can be used to alert residents within minutes of the incident to help limit the damages and reduce risk both for the insurer and the insured. IoT can also be used to help detect fraudulent claims. Insurers could determine if a property is outside the area damaged by a hailstorm by combining location information with IoT micro-weather reports.
- **Healthcare IoT**
  Health insurance: medical devices that prevent risks related to blood pressure or glucose levels are in the very early stages of development. In the U.S., early detection solutions for diabetes use identification of pre-diabetes factors and the costs are reimbursed by insurers. Early prevention helps to cap costs for insurers and potentially improves the health and extends lifespans of individuals.

The examples of IoT implementation cover only a fraction of sectors where insurance services are provided. Considering the overall growth rate potential of the market, insurers' product and technology departments will be compelled to develop novel uses for the technology.

3. Regulations and Practices

Compared to traditional consumer technology, safe and resilient internet-enabled devices require enhanced security approaches and measures. To protect business and consumers, security and privacy by design should be foundational elements of connected devices development and production.

As described in the chapter, 'What is IoT', the IoT is actually much more complex than non-connected products and involves entire ecosystems. There are different players in the IoT lifecycle: hardware manufacturers, operating system developers, firmware and software developers, app developers, cloud computing providers, etc.

For this reason, security measures need to be implemented by all the players in the value chain, ideally in an integrated fashion. However, organisations cannot always control the security measures of their suppliers. Security measures need to be available even when IoT products are no longer functional nor connected to IoT networks, since confidential information can still be retrieved from the device itself. As such, processes for risk assessment, identity management, data management, vulnerability monitoring, incident response, and more must be comprehensive and continuous, adapting to distinct and ever-evolving requirements for each stage of the IoT lifecycle.

Due to the nature of the IoT market, specific regulations have been developed for certain geographic areas or sectors. Below, there are notes on the main applicable European regulations.

It will be important to identify not only the regulations that are relevant from an insurance perspective, but also those applicable to the business environment or to customers that actually use the devices.

The main drivers affecting IoT applicable regulation, in addition to geography, are the following:

- Type of data handled: personal and certain sensitive data are specifically relevant.
- Market sector: certain sectors are subject to specific safety or consumer health regulation.
- Device type: the IoT is regulated itself.

The General Data Protection Regulation (GDPR) - EU Regulation 2016/679 is relevant also in the IoT field, since it introduces the concept of privacy-by-design. When an organisation intends to use an IoT solution, it should consider from the design stage: contractual clauses with suppliers; the need to inform data subjects about the collection and processing of data; and how to manage data access grants and revocation.

Various regulations have been (or are being) issued by European institutions to protect strategic sectors from IT risks and harmonise national legislations, like the NIS EU Directive 2016/1148, the Cybersecurity ACT 2019/881, the future Digital Operational Resilience Act (DORA). Although specific to certain sectors deemed critical, the NIS (Network and Information Security) Directive 2016/1148, designed to ensure a common level of minimum security, has implications also for the management of IoT.

In December 2020, the European Commission presented a proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), which includes further sectors in its scope, and expands the list of measures to be adopted in risk management process, which now includes controls on the cybersecurity of its suppliers or the use of cryptography. Complementing the NIS Directive, the Cybersecurity ACT 2019/881 establishes a mechanism for the creation of European information security certification systems for specific IT processes, products and services, in particular for the devices connected to the Internet. This regulation empowers ENISA (the European Union Agency for Cybersecurity) to set up and maintain the European cybersecurity certification framework. The agency is actually working on the first candidate cybersecurity certification scheme (EUCC), on an EU Cybersecurity Certification Scheme for Cloud Services, and an EU cybersecurity certification scheme for 5G networks.

Eight common thematic blocks underpin IoT security regulations developed across geographies and industries:

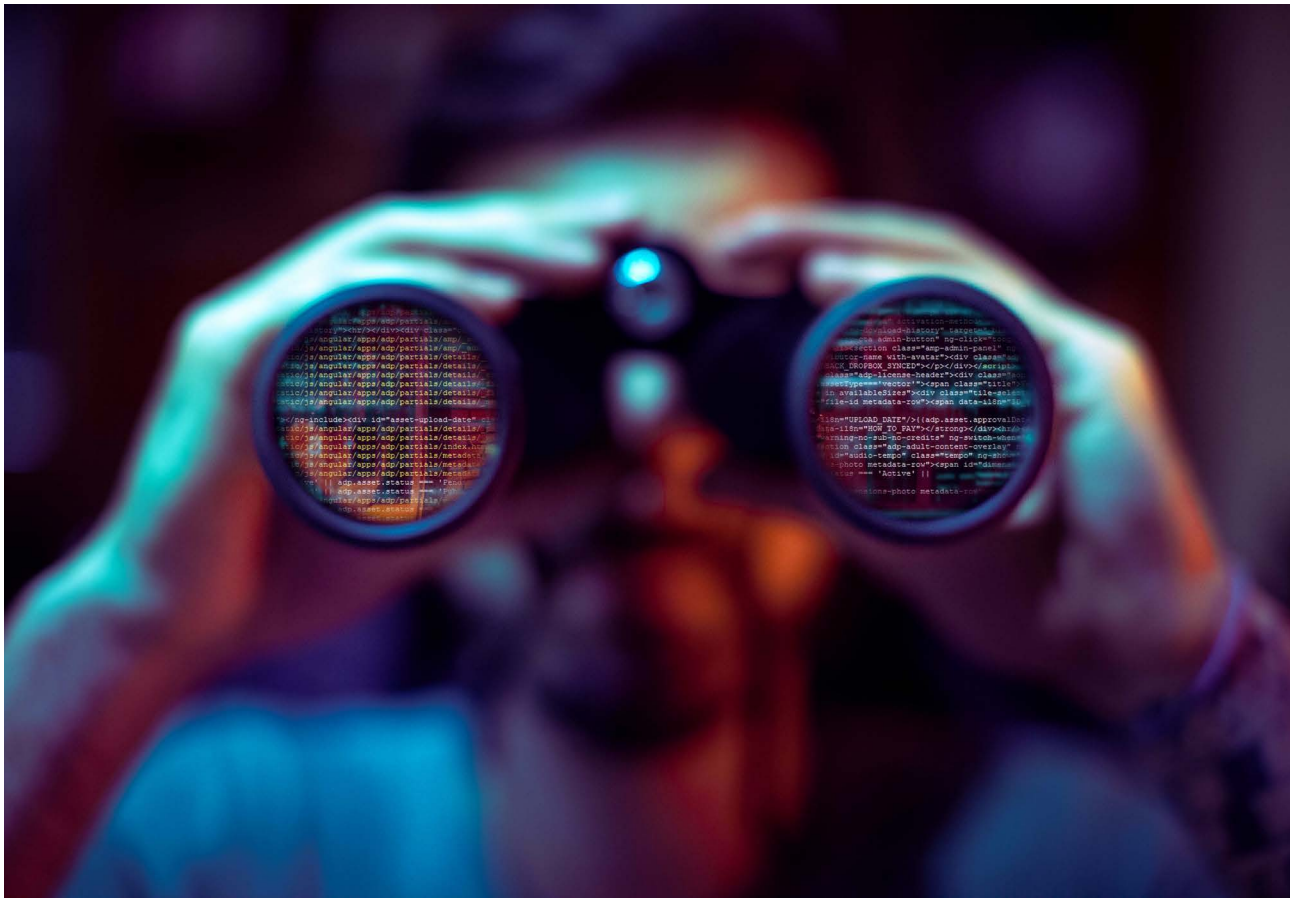
- governance
- risk management
- supply chain management
- secure development lifecycle
- configuration management
- identity management
- data management, and
- vulnerability management

ENISA works together with EU Member States and other stakeholders to deliver advice and solutions as well as improve their cybersecurity capabilities. It has been working on good practices for securing the IoT since 2016 by publishing studies that map the threat landscape and provide targeted security measures. The agency's key publications in this arena include Good Practices for Security of IoT - Secure Software Development Lifecycle, Industry 4.0 in the Context of Smart Manufacturing, Smart Cars, Smart Hospitals, Smart Airports. It also supports the development of a cooperative response to large-scale cross-border cybersecurity incidents or crises.

At the time of writing, DORA is a draft regulation by the European Commission part of the European Commission's wider Digital Finance Strategy to support the development of digital finance while mitigating associated risks. The proposal builds on existing information and communications technology (ICT) risk management requirements already developed by other EU institutions and ties together several initiatives into one regulation to create a harmonised approach across the EU, regulators and financial services industry. The draft introduces powers for financial supervisors to oversee risks stemming from financial entities' dependency on ICT third-party service providers (e.g., Cloud Computing). DORA regulates six key aspects in particular: governance; ICT risk management; ICT-related incident reporting; digital operational resilience testing; third-party risk management; and information sharing.

Since 2019, the European Telecommunications Standards Institute (ETSI) has been developing the ETSI TS 103 645 standard for the cybersecurity of consumer IoT products, and in June 2020 has released the ETSI EN 303 645 "Cyber Security for Consumer Internet of Things: Baseline Requirements". ETSI is the officially recognised body with a responsibility for the standardisation of Information and Communication Technologies (ICT), officially recognised by the European Union as a European Standards Organization (ESO). The standards developed by ESOs are the only ones that can be recognised as European Standards (ENs).

The ETSI EN 303 645 standard mainly regulates the safety of consumer devices and related services connected to the internet including: children's toys and baby monitors; connected safety-relevant products, such as smoke detectors and door locks; smart cameras; TVs and speakers; wearable health trackers; connected home automation and alarm systems; connected appliances (e.g., washing machines, fridges); and smart home assistants. This standard, which provides a basis for future IoT certification schemes, supports a good security baseline for connected consumer products, provisioning a set of 13 recommendations, with the top three being no default passwords, a vulnerability disclosure policy, and updated software.



Although this section focuses on the main regulations applicable in Europe, it should be noted that in some states of the USA (e.g., California and Oregon) there is 2019 regulation on IoT devices according to which manufacturers are required to equip IoT devices with reasonable minimum safety standards. At the US federal level, the "IoT Cybersecurity Improvement Act of 2020" aims to establish minimum security standards for IoT devices owned or controlled by the US federal government. The law aims to address cyber threats by leveraging the considerable purchasing power of the US government by pushing manufacturers to build secure devices from the design stage, with the support of NIST (US National Institute of Standards and Technology) issuing recommendations to ensure the safe development of devices. Among NIST publications, we note in particular the NIST IR 8228 - Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks (2019)", which outlines the security and privacy risks of IoT devices for the organisations using them.

The fundamental principles of cybersecurity and privacy (data management, identity management and risk management) remain however the backbone of trusted IoT products and provide a solid foundation for IoT device security.

In particular, for companies using IoT solutions are relevant the standards ISO / IEC 27001: 2013 Information security management systems and the ISO / IEC 27031 - Guidelines for information and communication technology readiness for business continuity. The first relates to data protection according to the principles of confidentiality, integrity, and availability defines a set of controls that can be applied to any organisation. The ISO / IEC 27031 provides indications to prevent an uncontrolled incident from becoming a threat to the operational continuity of an organisation. Compliance with these standards meets most of the requirements of other cybersecurity standards and guidelines.

In addition to the already mentioned ENISA, NIST, ETSI, and ISO / IEC, the Cloud Security Alliance (CSA) has published the "Internet of Things (IoT) Security Controls Framework Version 2" (2020), and the IoT Open Web Application Security Project (OWASP).

There is a quick run-up to the development of specific guidelines and standards across sectors, and in the absence of specific instructions for the IoT, general ICT rules are used. Certain sectors are also self-regulating in an effort to develop specific IoT security standards (through the Automotive

Information Sharing and Analysis Center "Auto-ISAC", the automotive industry is designing best practices to secure connected vehicles; the International Medical Device Regulators Forum is supporting the healthcare industry to improve the overall security of medical devices).

For the insurance sector specifically, are relevant the ICT Security and Governance Guidelines (October 2020) and the Guidelines on Outsourcing to Cloud Service Providers (February 2020) issued by EIOPA. The operational resilience of insurance and reinsurance companies with the aim of protecting the digital assets is pursued through detailed requirements in the areas of ICT Governance, Risk & Strategy, ICT Operations Security, ICT Operations Management, Business Continuity, and Supplier Management (including cloud providers).

Eight common thematic building blocks can be identified for an IoT security framework complying with regulatory requirements and best practices:

1. Governance
The definition of organisational policies, processes, roles and responsibilities is necessary to adequately address risk throughout the IoT lifecycle and ecosystem.

2. Risk management
A robust approach to risk management—which evaluates both immediate threats and potential threats that may emerge down the value chain—is the first step toward designing secure products and helping organisations understand where to focus security efforts.

3. Supply chain management
Suppliers play a part in designing, building, sourcing, and delivering hardware and software. Therefore, the use of IoT solutions requires verification of the security measures of third parties involved across the ecosystem, as physical and cyber threats can have an impact on continuity, and more generally on security.

4. Secure development lifecycle
IoT products should be designed end-to-end with security in mind—from prototyping to development to deployment, also with a view to achieve real long-term cost savings and operational efficiencies.

5. Configuration management
The root causes of many IoT device incidents have been tied to weaknesses in the devices' default settings or the ability to modify settings—intentionally or unintentionally—in a way that weakens their security.

6. Identity management authentication, and access control
Identity management, authentication, and access control ensure that the use of connected devices is limited to authorised people, processes, and devices.

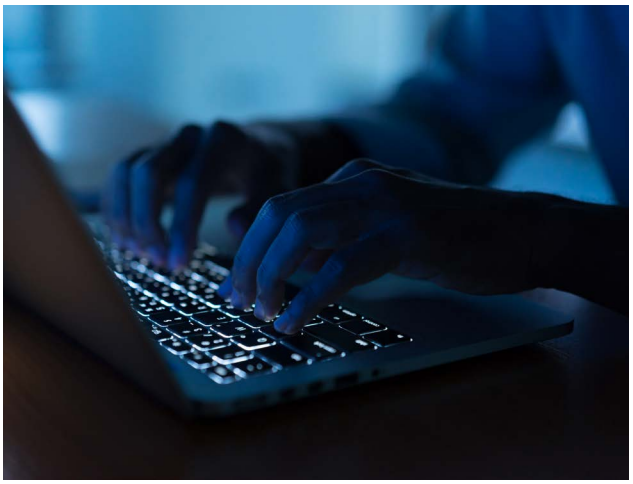
7. Data management and privacy
All the players in the IoT ecosystem are responsible for implementing reasonable methods to protect data that is generated, collected, stored, and transmitted from/to connected devices.

8. Vulnerability monitoring, management, patching, and response
Most IT risks can manifest after an IoT product is released. From malware to ransomware to eavesdropping, threats to software and hardware are evolving each day as malicious actors launch more and more sophisticated attacks. To mitigate risks as they arise, manufacturers and service providers are expected to actively and continually monitor, identify, and fix security problems in IoT devices, including those in operation.

4. Main Risk Areas

4.1 Cybersecurity

Extensive use of interconnected online devices naturally raises cybersecurity risks concerns, as each individual object may be leveraged as the "weakest link" in the IT chain for cybercrime purposes. Connected devices are generally less closely monitored compared to more traditional IT systems, creating potential exposure to cyberattacks. This stems from the fact that connected device manufacturers may maintain closed-source systems that make it hard for owners to update, maintain and fix security issues – getting detailed specifications and knowledge of the embedded hardware and software components can even be difficult. In addition, less effort may be spent on making hardened devices, to keep production costs under control. Finally, manufacturers tend to consider IoT devices as "things" rather than "computing devices". For this reason, sometimes little concern is given to providing software update and security fixes all along the device's life cycle once it is off the shelves. And as these devices may be targeted to retail markets, in the sake of "ease of use" connected objects often come pre-configured with default, identical authentication parameters (admin credentials, configuration interface URL...). An additional layer of complexity in assessing cybersecurity risks is involved when the device's data flows through the manufacturer's or another third-party's cloud services before being accessible by the end-user.



The main weaknesses associated with IoT use with respect to cybersecurity risks include:

- **Insufficient data protection:** the data collected and processed by the device shall be protected by a layer of encryption, relying on strong algorithms and complex keys. Yet, the device user is not always able to gain comfort over the actual security deployed by the manufacturer. If the device user does not have full control over encryption keys and algorithms, there is a risk that a third-party could access data.
- **Insecure network services:** a poor (or inexistant) encryption solution of the data in transit over the network exposes the device's data. As per stored data, encryption shall rest on strong algorithms and keys to safekeep confidentiality of exchanges. The device configuration should limit the number of open ports to a minimum, as well as active network protocols, to avoid unwanted remote interaction with the device.

Connected devices have an impact on the insurer's risk exposure, whether he relies on IoT to collect data for insurance purposes or extends cover to clients who are themselves device owners. Aside from the obvious cybersecurity risk that calls for specific countermeasures, the insurance company must also consider strategic and reputational risks involved, as well as risk accumulation linked to the very nature of connected devices.

- **Inefficient Patch management:** lack of updates, or insufficiently secure configuration from the get-go, may expose the device to attacks. These attacks can leverage on unfixed bugs in the software. Lack of update may also lead to insecure software stack. These can be exploited, especially when there is a web admin interface.
- **Unnecessary storage or transmission of personal data:** specific care needs to be taken to limit personal data stored on the device or transmitted by it. Unless the user can perform depersonalisation of data, de-associating personal identifiers from datasets, the user is

Illustrative example: hacking a PAYD box

Pay as you drive (PAYD) insurance requires the insurer to assess mileage for premium adjustment. To do so, the insured car is equipped with a device that will submit mileage data (possibly alongside other driver behaviour-related data) to the insurance company. If the device is compromised, the data can be tampered with, sending wrong information about the insured's risk profile and distorting premium calculation.

taking the risk that personal information could be revealed in case the data is intercepted by a third-party. Generally speaking, data collection should be limited to the user's actual needs.

- **Weak authentication:** use of manufacturer-defined logins, with limited rules for password complexity, or even pre-defined, standard, passwords, including admin accounts with extended privileges, make it easier for cybercriminals to tinker with the device, especially if it allows for remote access over the internet. Even if there is no predefined password, users generally pay less consideration to IoT compared to "real" computers, and thus may choose overtly simple password that are more susceptible to brute force or dictionary attacks.

All these weaknesses open possible pathways for attackers. Attack scenarios to be considered relate mostly to remote attacks, yet in some, rarer cases, physically laying hands on the device can lead to possible intrusion. Main attack scenarios for consideration are as follows:

- **Denial of service:** taking advantage of open ports for external communication, and the generally limited computing power associated with the device, an attacker can disrupt its ability to function by flooding it with requests. Such attack can be considered less worrying, as it does not aim at taking control of the device itself or access its data, yet they practically make the device unresponsive. That may be an issue if said device is of critical importance to the user or to other systems connected to it.
- **Unauthorised access to the device's stored data:** through a combination of open remote access ports, and login/password cracking (taking advantage of possible weaknesses in the authentication process), an attacker can get read and/or write access to the data stored on the device. That access can then be leveraged upon to steal the data or encrypt it in a ransomware attack.
- **Unauthorised access to the device's operating system:** if the remote access granted through password cracking is associated with admin privileges, the attacker is now able to perform changes in the software itself. Apart from erasing the system and data entirely, the attacker has the opportunity of installing software of its own that may change the behaviour of the device. In this instance, it is also possible to turn the device into part of a botnet that will be implicated in further malicious attacks.
- **Snooping on dataflow:** in this scenario, insufficiently secure network communications open the way for an attacker to intercept the flow of data, being able to read it.
- **Man-in-the-middle attack:** an attacker may not only intercept the flow of data between the device and the server it is connected to but may also modify the communication between the server and the device by "impersonating" the server in communicating with the device and doing the same with the server. In this instance, it is possible to generate fake data on the server or affect the behavior of the device.

Illustrative example #2: healthcare IoT

Hospitals and healthcare organisations rely on a very diverse range of online devices collecting data from patients. The sheer diversity of the equipment makes it hard to enforce proper security measures. As a result, it is estimated that a significant number of organisations may be exposed to serious risks of remote code execution and hacking (source: ITHealthSecurity.com).

From an insurance perspective, a cyberattack targeting medical devices could trigger significant claims, if eventual damages to clients were to be covered by the medical liability insurance policy.

The relative scarcity of computing power and memory allocated to connected objects limits the ability to deploy security countermeasures, which are generally based on computer-intensive algorithms. In case the device also relies on a third-party cloud services, these may be targeted by an attacker. Even though cloud infrastructure can generally be considered more secure than IoT devices, it still can be subject to attacks, with consequences to all connected devices at once.

The consequences of the attacks can thus range from loss of data to complete loss of control of the device and potential supply chain disruption. If the information collected by the device is

dependent upon by other systems (for example, health or industrial monitoring systems with alarm notifications if measures reach critical levels), the attack can ricochet on larger processes with significant consequences. If the data processed by the device is considered sensitive, any breach is a major concern. Any device with actuators (servomotor for example) can be used by the attacker to also perform actions on the physical world; connected locks are a clear illustration of this. Getting control of the device also creates the risk of using it as a gateway into the other parts of the network, paving the way for larger-scale attacks.

4.2 Strategic and Reputational Risk

The shortage in resource mentioned in paragraph 3.1.1 impacts the IoT production and therefore could slow down the digitalisation of Insurance companies.

Indeed, the shortening of consumer devices, smartphones, and tablet will slow down the transformation the insurance industry is embracing to simplify the customer journey leveraging on 5G, smart devices, IoT, AI, Big Data, and other technologies, which depend on the availability of rare-earth minerals. In case of a sudden tightening of USA-China relationship and the subsequent interruption of the supply of these materials, the insurers digital strategy would be undermined. Indeed, the supply interruption would increase the cost of digital devices, causing an inversion to legacy processes (i.e., underwriting/claims management paper-based), and a drop in demand of devices/sensors for smart house/car/health insurance, needed to assess risks, and offer a tailored coverage to the costumers.

Therefore, the insurance industry needs to properly assess the risks related to rare earth materials, not only from a technological point of view, but also considering the related impact on its business strategy.

Also, at a time when ESG is a hot topic, insurers should consider the reputational risks associated with the use of IoT which rely on mining activities. In particular, proper due diligence of the IoT supplier or IoT component supplier should be performed.

Rare earth demand and mining related risks:

In 2019 the total global demand for rare earth oxides (REOs) has been 208,250 metric tons and is expected to increase to a forecasted 304,678 metric tons by 2025, driven by the increasing uptake in green technologies and advanced electronics. This creates pressure on global production.

Rare-earth metals are currently extracted through mining, which comes with several downsides and risks, including on the environment:

- Mining for rare earth minerals generates large volumes of toxic and radioactive by-products, due to the co-extraction of thorium and uranium — radioactive metals with known adverse effects on the environment and human health,
- Mining, processing, and disposal can contribute to ecosystem disruption and the release of hazardous by-products into the atmosphere,
- Mining is water-intensive, which is worrying, given the dwindling fresh water supply as the global warming continues to change global weather patterns.

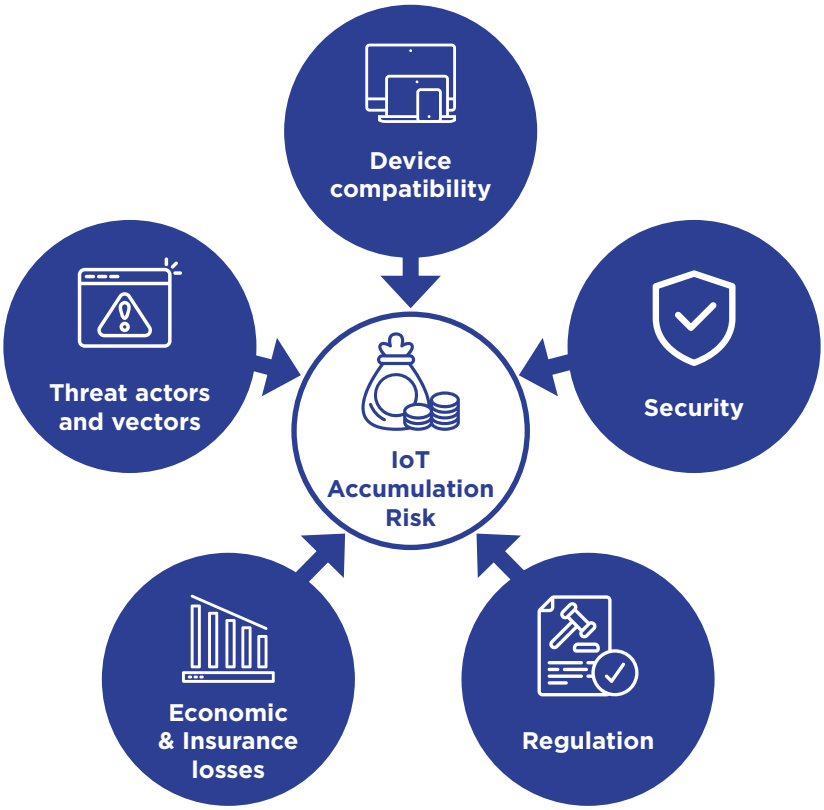
4.3 Accumulation risks

Perhaps one of the most crucial aspects to understand when considering the new IoT risk is the possibility to have an accumulation event. As we've seen with the new cyber risks, the losses are not geographically restricted and have the capabilities to impact a wide range of location, industries, and ecosystems. The accumulation risk associated to IoT should not only be restricted to new product offerings, but also to existing products which could contribute to losses. Given that IoT devices communicate one another and are capable of self-configuring it will be needed to understand if this feature contributes to bring greater risk of a catastrophic accumulation event for the (re) insurance market. Some IoT aspects to consider in assessing the accumulation potential include:

- **Compatibility:** Can devices communicate between brands sufficiently well to avoid brand competition? If one brand becomes dominant could this risk change?
- **Security:** Is the security on devices safe enough to prevent an accumulation event or is it so weak that its likely to enable systemic events and insurance losses?
- **Regulation:** Is regulation (and corporate responsibility) sufficient to prevent unnecessary storage and accumulation of personal/sensitive data?
- **Insurance loss:** Would the potential events from IoT risks translate to economic material and subsequent insured losses?
- **Threats:** Do threat actors have the motivation and resources to perform an attack through an IoT system or would an IoT system provide a new attack vector for a systemic event?

Ultimately (re)insurers need to get comfortable on accepting the accumulation risk associated with IoT. In order to do so, quantification approaches will need to be developed and exploited by the existing cyber insurance market. Understanding the common vulnerabilities that would result in systemic losses is crucial in being able to manage the risk and capital support. Crucially, if IoT devices are "self-adapting" and dynamic, the challenge becomes in developing an accumulation approach that also cohabits with this risk. On the next page, is reported an accumulation risk scenario that could be useful to understand the risks that the re-insurer needs to manage.

Figure 5: IoT Accumulation Risk



Accumulation risk scenario:

A critical vulnerability in a software library is discovered which is massively used in all kinds of commonly used applications and services across the internet. If left unfixed, threat actors with malicious intent can break into systems, steal passwords and logins, extract data, and infect networks with malicious software.

The vulnerability requires very little expertise to exploit and within 24 hours multiple ways of exploiting the vulnerability becomes publicly available making organisations and end-users vulnerable to cyber-attacks.

Because of the critical nature, widespread and easy exploitation, there is a high risk of cyber-attacks affecting business processing and compromising data. Due to the increasingly linking of operations and infrastructure to complex hyper-connected environments, including Internet of Things, there is a high risk of a systemic cyber event causing a breakdown of an entire sector or multiple sectors.

This type of event has the potential to impact various areas of coverage, standard cyber coverages related to data breach, recovery costs and liability are likely. Furthermore, possible secondary coverage losses related to IoT device compromise could result in losses to:

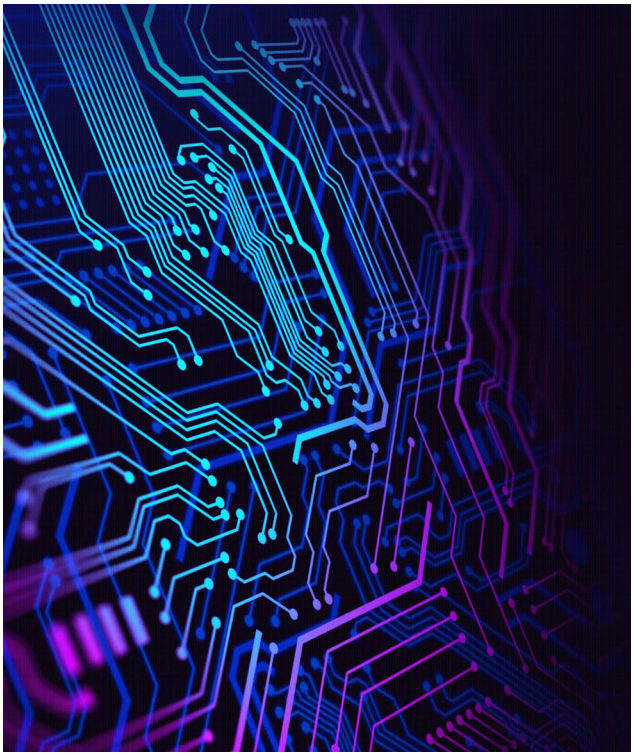
- Accident & health and Life where IoT devices are used to manage a patient wellbeing.
- (Contingent) Business Interruption where the IoT devices are critical as the manufacturing and or supply of good and services thus resulting in a supply chain issues
- Errors and Omissions where the IoT provider has failed to adequately secure the devices
- D&O coverage for specific cases of professional negligence related to the use or deployment of IoTs.
- Property losses are possible if the IoT dependency failure results in a physical damage (although policy wordings may adequately manage this)
- Any coverage triggering as a result of global economic instability as a result of a catastrophic systemic cyber-attack e.g., credit & surety, could results in losses.

The above list is a example of some coverages that could be at risk depending on the scale and nature of the event. Whilst the impacts on various coverages would likely differ in severity, the secondary impacts from such an event are very likely and it is currently unclear if existing policy wordings would be sufficient to mitigate the losses.

An example of such critical vulnerability with high impact is “Log4shell” discovered in Q4 2021 which is potentially the most severe computer vulnerability in years.

As the IoT landscape continues to emerge (re) insurers need to consider as many aggregation events as possible, drawing from near misses to the theoretical, to ensure they are comfortable and able to absorb the risk transfer.

Given how rapidly this risk is growing, it is important that a risk management framework is developed to help all areas of the business understand and communicate the emerging risk. This includes underwriters across all lines of business, to claims teams and ultimately senior management and the board.



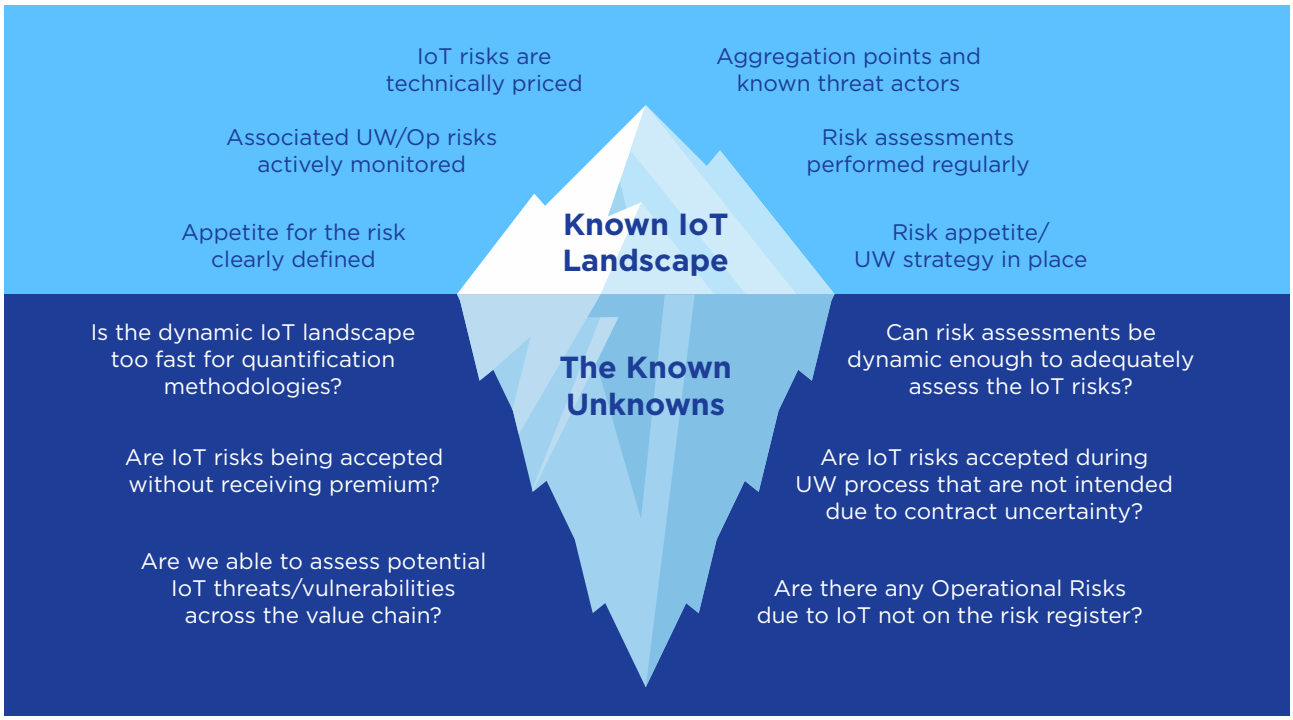
5. Risk Management and Capital

With the rise of interconnected online devices insurers must develop an approach whereby they can manage/monitor and ultimately quantify the risks associated. This concept is not new for the insurance market and it has been recently developed by the cyber insurance market. As with any developing risk and/or product area there will be a journey in order to understand the full extent of the risk and to some degree if IoT devices are "self-adapting" and dynamic, but there may always be some unknown risks as the iceberg diagram displays. A good risk management process for evaluating IoT risks would include:

- **Risk Appetite Statement:** The company should define and clearly document its appetite for accepting IoT risk in the products that it offers and as part of the operational risks. Some of the risks will be unavoidable and, in these cases, adequate measures to mitigate the risk to an acceptable level for the company's risk appetite need to be defined.
- **Quantification:** The risks associated to IoT should be quantified, if possible. Through this approach the risks can be technically priced and monitored in a measurable way covering both the underwriting and operational risks the company faces.
- **Risk Assessments:** Risk management should perform regular risk assessment of its exposure and management of the IoT risks. This should include how well the accumulation risks are understood and managed.

"The Known Unknowns" displayed within the figures above, represents the challenges for the (re) insurance industry. In particular, one element which should be challenging is ensuring that the contract wordings are sufficient to avoid the acceptance of a risk, which should not be foreseen during the underwriting process.

Figure 6: The Known Unknowns



5.1 Operational and Cyber Risk Mitigation

Jointly with the risks arising from the underwriting process, (re)insurers will also need to be aware of any new operational risks that affect the business. These risks should be captured on the company's risk register and properly assessed. Depending on the (re)insurers business model there will be different levels of exposure to IoT in their operational risk. The operational risk assessment will need to ultimately determine if the risk requires mitigation actions and if the controls already in place to manage the risk are sufficient. Companies may also need to consider if the growth of IoT increases or reduces the frequency and/or severity of existing risks on their register. Ultimately, it is necessary to consider if IoT brings amendments to the operational risk framework.

The insurer's response to aforementioned threats depends on whether the covers it extends may include connected devices with an impact on potential claim occurrence and/or severity, or if it is itself relying on connected devices in order to carry service.

The rise of IoT presents new challenges for (Re) insurers in how they manage and control the risk. They need to develop their risk management approaches to understand and manage the IoT risks across the business.

5.1.1 Connected devices included in a policy cover

In the context of an insurance cover extended to clients, either retail or professional, risk exposure can be limited through setting policy deductibles, limits, and/or exclusions. A review of current risk exposure is required to identify possible "silent covers". The insurer can then either:

- replace silent covers with explicit covers including specific deductibles and sub limits (and funded by an appropriate premium), or,
- add a specific exclusion for damage caused by cyberattacks targeted at connected devices, or,
- leave the policies unchanged and take the increase in risk exposure into account when assessing the line of business' expected profit and volatility.

Of course, making such a change to the policies may not always be this simple, especially with industrial or professional clients: aside from the potential premium increase that they would face, such devices may be critical components in their activities. As such, customers would not accept to exclude these assets from their covers. We can cite as examples healthcare facilities with widespread use of connected medical devices, or plants relying on factory floor control devices.

In this instance, an insurer could focus on risk prevention, by requiring that its clients undertake fundamental security measures to ensure devices in use do not present an unacceptable security risk. Such measures should be part of the clients' risk management approach, and could include:

- hardware specification reviews and/or code audits for vulnerability assessment,
- control of their vendors' service level agreements:
  - IoT suppliers should commit to regular software updates along their product's lifecycle,
  - vendors should also share the results of vulnerability analyses, to provide assurance on product safety,
  - whenever possible, include a vendor warranty covering possible costs associated with damage due to insufficient hardening of the device attributable to the vendor.

5.1.2 Connected devices deployed by the insurer

When the insurance company relies on a connected device to provide services to policyholders, it must exercise proper due diligence during vendor selection to ensure adequate security is enforced. The requirements made to clients are generally applicable, yet more in-depth examination is needed.

Best practices in terms of connected device specifications include, yet are not restricted to, the following aspects:

- **Hardware specifications allow for future software updates** and application of algorithmic security measures: while cost consideration could push the vendor to provide "just the right amount" of resources for the device to work out-of-the-box, capacities should not be restricted to the point that available memory or computing power could prove insufficient to support updates within the expected lifespan of the product or require a scaling-down of security measures so that it is usable.
- **Operating system and software rely on well known, tried-and-tested standard components:** insurers shall as much as possibly avoid reliance on opaque, lesser-known software whose security is less scrutinised. This also includes use of standard secure network communication protocols.

- **Vendor commits to regular security updates** along the product's lifecycle, and reports on possible vulnerabilities identified. Updates shall also include firmware components.
- **Volatile and non-volatile data is protected using cryptographic algorithms and encryption key lengths which meet minimal standard requirements**, such as FIPS' Advanced Encryption Standard or comparable standards. If public key cryptography is used, private keys should be generated on the device using sufficient entropy, and not be exposed.
- **Services and open communication ports are strictly limited** to what is necessary for device operation.
- **Users' access rights are strictly limited.**
- **Authentication is required and relies on strong mechanisms.**

In addition to these considerations, the insurance company needs to perform a thorough review of the impact the use of connected devices will have on its IT environment and assess the security requirements accordingly. The first line of defence against IoT security failure relies on appropriate network segmentation.

Even though the device may be considered secure enough from a software perspective, there is still a risk that users may try to hack into it and affect its behaviour. To counter this type of insurance fraud attempts, physical protection of the device needs to be considered. For example, access to the PCB could be protected, with cover exclusion in case a device examination reveals evidence of tampering. Additionally, debugging or flashing modes should not be available to end-users.

5.2 Underwriting and Cybersecurity risk mitigation

5.2.1 Risk Selection

Development of a clear underwriting strategy that identifies the type of IoT risks that a company is prepared to accept is crucial. A clear and defined risk appetite that is understood both by the underwriters and at the board level will likely need to be developed to adequately manage the risks that need to be accepted. The growth of IoT will undoubtedly lead to the development of new products to cover the new risks faced by embedding the technology. MGA may lead with specialisms in the risk assessment for these new products and these will need to be supported by the (re)insurance market. For both existing and new products, the risk assessment will need to be supported by the development of technical pricing tools that attempt to quantify the IoT risk:

- **Existing Products:** Pricing actuaries will need to consider how the IoT developments impact existing business lines and how they can incorporate that within their pricing methodologies. Risk assessments can help in identifying these risks on existing business lines and support the development of quantification methods. Each business line will be affected differently and to a different extent. For example, in some business lines the underlying risks are increasingly relying on interconnected devices to change the way risks and losses materialise. This assessment will essentially evaluate how existing coverages are impacted by the rise in IoT.
- **New Products:** The developments of new products related to IoT may be a new opportunity for the insurance market in the future to provide cover to clients facing new risks.

Quantifying and pricing these risks will follow the same guiding principles of assessing the IoT risks to current business lines but the focus will be narrower to a more clearly defined product and coverage.

For any risk selection process is necessary to consider its related risk portfolio. Hence, it's fundamental to capture the relevant data to monitor the risk selections, in order to make comparisons to the risk appetite statement. This will likely require new data points for risks to be captured or augmented to enable analysis of the portfolio.

Earlier in this paper some opportunities were outlined for the use cases of IoT including; wearables; healthcare; smart ecosystems; and artificial intelligence. As the market grows with innovative insurance product offerings each company will have to assess its appetite for these new risks. Particularly complex underlying risks such as AI, may require additional expertise within the company in order to fully understand the risks involved in such products' offering. Therefore, it is likely that some companies would feel more comfortable hiring experts from these fields who have a deep understanding of the risks to underwrite these new products.

5.2.2 Catastrophe Risk

The underwriting risk framework should consider the potential for catastrophe risk arising both from new and existing products. Each company will need to define its risk appetite for this catastrophe risk and communicate this across the company. At present it is difficult to know the true extent of any IoT related catastrophe event and what implications if may have. It is possible that a truly catastrophic event may also impact the global economy. In which case, attaching return periods to these events will continue to be challenging and rely largely on expert judgements. For this purpose, working closely with cyber security and IoT experts will be important so that the risk potential is fully understood and the company manages its catastrophe risk appropriately. Overtime it is likely modelling companies will offer solutions as the demand for the technology and the risk in the (re) insurance market grows.

5.3 Underwriting risk mitigation

To manage and mitigate the risk (re)insurers will use risk transfer mechanisms and purchase reinsurance programs to suit their risk appetite. In order to enable the required capacity in the market to perform this risk transfer, the risk must be adequately understood and quantified to be able to transfer the risk efficiently. Supporting the growth of new IoT products may take time as the (re)insurance market develops it's understanding of the risks. Alternative risk transfer mechanism may also be available, as the ILS products, so that some of the risk can be transferred to the capital markets, but again the risk would need to be adequately quantified and an appropriate independent and measurable trigger defined.

5.4 Capital Impacts

(Re)insurers will need to consider to what degree the growth of the IoT market impacts their capital requirements and if it requires additional capital to be held to cover this risk. For what concerns capital, this will generally focus on the risk's impact on the tail of the business's capital distribution and if it's a material contributor. (Re)insurers will need to consider the impacts of potential correlations of IoT events across their portfolios and across risk types, considering that they have the potential to impact various business lines and produce global economic implications. If the analysed risk is related to business and also included in the ORSA, stress and scenario analysis may be required to understand the capital and solvency strain for various types of IoT events. Capital implications may also be influenced by the regulators and credit rating agencies on the basis of their view of the IoT risk. For some (re) insurers IoT products may provide another tool through which diversify their portfolio and for others it may create additional concentrations and correlations of risk. Hence, the impact of capital will vary depending on the business model and on the ability to hedge the risk via risk transfer mechanisms.

(Re)insurers must establish to what extent they are willing to accept the change of IoT risks and make the proper changes to their business model if required. However, to be able to make an informed decision on this topic, the company must understand the risk and its implications and communicate it to the board, in order to take a decision on their risk appetite. This will be challenging as it's a complex and fast-moving environment where new way of looking at the risk may need to be developed. This may require more dynamic ways of looking at the risk than the industry has been traditionally used to. IoT will change the risk landscape of many products and bring new opportunities for developing innovative profit. The industry must be ready to react and understand these risks to navigate the growth of IoT on an ever increasingly connected world.

Conclusions

Humanity has always sought ways to bring predictability to the apparently chaotic physical world, to understand and to gain control over it. Of the most significant inventions of the XX century, no other embodies those goals better than digital computing. It comes as no surprise, that ever since the advent of modern computers, inventors have been trying to bridge the gap between the physical and digital worlds to reap the advantages of the former – measurability, clear causality, and control over interactions.

In the past decade, the capabilities of semiconductor components and wireless technologies have been steadily increasing, while the price/performance ratio has been becoming ever more attractive. Nowadays, we have reached the stage in which the buildings we live and work in, vehicles we travel in, and even daily use items are seeing their functionality extended by the integration of integrated circuits and sensors.

Given the presence of digitally enabled, interconnected, sensor-rich objects in our professional and private lives, we can safely say that the concept of Internet of Things went from the drawing board to mass adoption.

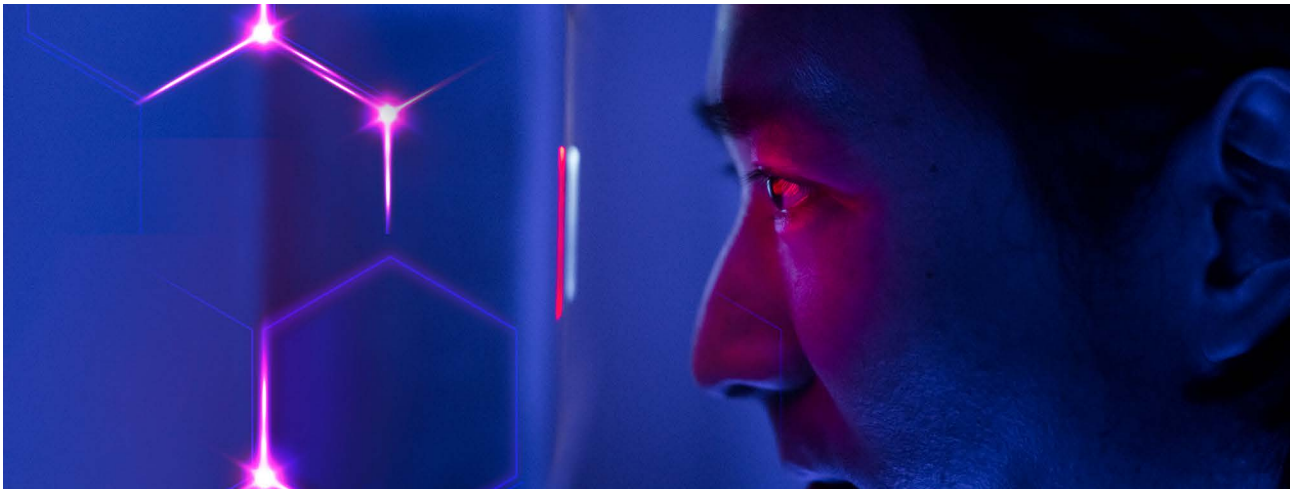
Before trying to dive deep into the details of the trend, we first needed to understand its scope. In fact, we have discovered that the term IoT transcends just the physical component. The solutions we have analysed are built on four pillars - Devices (Sensors and actuators), Communication networks, Analytics and the Application layer. In terms of their presence, we have explored the key areas of their application - industrial, commercial, healthcare, transportation, and consumer.

Given the broad spectrum of applications and ever-increasing capabilities of devices and platforms, very favourable scenarios are forecasted for the IoT market. The global market size is expected to grow five-fold from 2019 levels to reach $1,500 billion in 2027. At the same time, the number of IoT devices worldwide is expected to almost triple in 2030, amounting to over 24.1 billion IoT devices.

As with every advancement in information technology, especially of this magnitude, care needs to be taken for the technology not to be misused. For this very reason, IoT security regulations have been developed across geographies and industries. As discussed, their aim is to introduce best practices in the areas of governance, risk management, supply chain management, secure development lifecycle, configuration management, identity management, data management, and vulnerability management.

We have also explored how adequate attention needs to be lent to this subject from the perspective of the insurance industry. Whether relying on IoT to collect data for insurance purposes or extending cover to clients who are themselves device owners, an insurer must understand and quantify the inherent risks of this technology. It is worth noting that the analysis must go beyond just the cybersecurity risk, also to include strategic, reputational and accumulation risks related to the connected devices.

To summarise, IoT presents new challenges for (re) insurers in how they manage and control the risk. A careful rethinking of the risk management approach to understand and manage the IoT risks across the business is needed.



References

1. What is IoT

- ENISA publications “Good Practice for IOT” 2017-2019 for IoT history, and type of IoT
- IEEE (Institute of Electrical and Electronics Engineers) published a document in 2015 Towards Definition Internet of Things, maybe there are some interesting points for history and background: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf
- ISACA Assessing IoT: for the IoT architecture paragraph
- Italian Association for Information Security (CLUSIT): 2020 publication “IoT Security e Compliance”: history, type of IoT and IoT Architecture
- ITU “Overview of the Internet of things”: definition of IOT and IOT Architecture
- NIST in its document NISTIR 8228 “Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks”, there is a chapter relating IoT Capabilities
- NIST Internet of Things (IoT) Trust Concerns (Draft): definition, risk areas
- https://www.nist.gov/internet-things-iot
- https://www.nist.gov/news-events/news/2020/12/nist-releases-draft-guidance-internet-things-device-cybersecurity
- https://www.mckinsey.com/industries/financial-services/our-insights/digital-ecosystems-for-insurers-opportunities-through-the-internet-of-things
- https://ubidots.com/blog/iot-consumer-vs-commercial-vs-industrial-main-overview/
- How the Internet of Things is reshaping business models in insurance, Geneva Association, May 2021
- Oracle. “What is IoT?” n.d. Oracle. 31 08 2021. https://www.oracle.com/internet-of-things/what-is-iot/.
- IERC http://www.internet-of-things-research.eu/about_iot.htm
- https://www.bbc.com/future/article/20140516-i-operate-on-people-400km-away

2. Market Analysis

- D, Ajay. “Industrial Internet of Things (IoT) Market to Grow at A CAGR of 21.3% During 2020 To 2028; Quince Market Insights.” 29 August 2020. Quince Market Insights. 16 August 2021. https://www.globenewswire.com/news-release/2020/08/29/2085754/0/en/Industrial-Internet-of-Things-IoT-Market-To-Grow-At-A-CAGR-of-21-3-During-2020-To-2028-Quince-Market-Insights.html.
- Fortune Business Insights. “Internet of Things (IoT) Market Worth USD 1463.19 Billion by 2027 Backed by Rising Awareness Regarding Precision Farming to Aid Market Growth, says Fortune Business Insights™.” 11 May 2021. Fortune Business Insights. 30 August 2021. https://www.globenewswire.com/news-release/2021/05/11/2227081/0/en/Internet-of-Things-IoT-Market-Worth-USD-1463-19-Billion-by-2027-Backed-by-Rising-Awareness-Regarding-Precision-Farming-to-Aid-Market-Growth-says-Fortune-Business-Insights.html.
- Ghosh, Iman. “4 key areas where AI and IoT are being combined.” 15 03 2021. weforum.org. 30 08 2021. https://www.weforum.org/agenda/2021/03/ai-is-fusing-with-the-internet-of-things-to-create-new-technology-innovations/.
- Holst, Arne. “Number of IoT connected devices worldwide 2019-2030.” 25 08 2021. Statista.com. 30 08 2021. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.
- IANS. “China to surpass US to become world’s largest IoT market in 2024: Report.” 17 January 2021. business-standard.com. 30 August 2021. https://www.business-standard.com/article/international/china-to-surpass-us-to-become-world-s-largest-iot-market-in-2024-report-121011700382_1.html.
- Lee, Yen Nee. “2 charts show how much the world depends on Taiwan for semiconductors.” 15 03 2021. CNBC.com. 31 08 2021. https://www.cnbc.com/2021/03/16/2-charts-show-how-much-the-world-depends-on-taiwan-for-semiconductors.html.
- Lueth, Knud Lasse. “Top 10 IoT applications in 2020.” 8 July 2020. IOT Analytics. https://iot-analytics.com/top-10-iot-applications-in-2020/.

- Novicio, Trish. “15 Biggest Semiconductor Companies in the World.” 06 01 2021. Yahoo Finance. 31 08 2021. https://finance.yahoo.com/news/15-biggest-semiconductor-companies-world-183721644.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAFy6zBUmliBwDsmQbdcHkeXPvlsXsCigyZYEJ9kJXmZaYnqQU6bVFvJIBSFifrwNMv0w9OCrEWzKK53-Vm8WZ7_.
- Oracle. “What is IoT?” n.d. Oracle. 31 08 2021. https://www.oracle.com/internet-of-things/what-is-iot/.
- Rotaru, Alexandra and Gabriele Roberti. “European IoT Spending to Exceed $200 Billion in 2021 as Companies Start Moving to the Next Stage of Recovery, according to IDC.” 09 June 2021. IDC.com. 30 August 2021. https://www.idc.com/getdoc.jsp?containerId=prEUR147929621.
- Transforma Insights. “Global IoT market to grow to 24.1 billion devices in 2030, generating $1.5 trillion annual revenue.” 19 May 2020. Transforma Insights. https://transformainsights.com/news/iot-market-24-billion-usd15-trillion-revenue-2030.
- Reuters. https://www.reuters.com/article/chips-shortage-explainer-int-idUSKBN2BN30J.
- The Conservation. https://theconversation.com/demand-for-rare-earth-metals-is-skyrocketing-so-were-creating-a-safer-cleaner-way-to-recover-them-from-old-phones-and-laptops-141360.
- Reuters. https://www.reuters.com/article/us-usa-china-rareearth-explainer-idUSKCN1T00EK.
- CNBC. https://www.cnbc.com/2021/04/17/the-new-us-plan-to-rival-chinas-dominance-in-rare-earth-metals.html.
- Statista. https://www.statista.com/statistics/1114638/global-rare-earth-oxide-demand/
- China University of Geoscience “Geoscience Frontiers”. https://www.journals.elsevier.com/geoscience-frontiers.
- Rigado. “Commercial IoT is Different” 13 August 2018. https://www.rigado.com/commercial-iot-is-different.
- Ubidots “IoT: Consumer & Commercial vs. Industrial - Main overview” 17 July 2019 <Ubidots IoT: Consumer & Commercial vs. Industrial - Main overview (ubidots.com)>
- Information security forum”Securing the IoT Taming the connected world” May 2019. https://www.securityforum.org/solutions-and-insights/securing-the-iot-taming-the-connected-world.
- Emergen Research “Internet of Things (IoT) Insurance Market by Insurance Type, By Application (Connected Home, Connected Car, Connected Health, Commercial Lines, Others), By End-Use (Automotive, Retail, Industrial, Residential, Healthcare, Logistics, Others), and By Region, Forecast to 2028” Jan 2021. https://www.emergenresearch.com/industry-report/internet-of-things-insurance-market.
- The Geneva Association “From Risk Transfer to Risk Prevention”. https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/iot_insurance_research_report.pdf.
- Mckinsey “Digital ecosystems for insurers: Opportunities through the Internet of Things” 4 February 2019. https://www.mckinsey.com/industries/financial-services/our-insights/digital-ecosystems-for-insurers-opportunities-through-the-internet-of-things.
- IBM “Disruption in the insurance industry”. https://www.ibm.com/downloads/cas/WVG1BPYW.
- Mordor Intelligence. https://www.mordorintelligence.com/industry-reports/internet-of-things-moving-towards-a-smarter-tomorrow-market-industry
- American Geoscience Institute. https://www.americangeosciences.org/critical-issues/faq/what-are-rare-earth-elements-and-why-are-they-important.
- GlobeNewswire. https://www.globenewswire.com/news-release/2020/08/29/2085754/0/en/Industrial-Internet-of-Things-IoT-Market-To-Grow-At-A-CAGR-of-21-3-During-2020-To-2028-Quince-Market-Insights.html.
- Reuters. https://www.reuters.com/technology/exclusive-ukraine-halts-half-worlds-neon-output-chips-clouding-outlook-2022-03-11/.

3. Regulation

- https://www.enisa.europa.eu/
- https://www.govtech.com/policy/state-lawmakers-go-after-iot-security-risks-contributed.html
- https://aioti.eu/wp-content/uploads/2019/06/DCMS_Mapping_of_IoT__Security_Recommendations_Guidance_and_Standards_to_CoP_Oct_2018.pdf
- https://iotsecuritymapping.uk/

- https://iotsecurity.clusit.it/#/ (Italian Association for Information Security)
- https://advisory.kpmg.us/articles/2020/rainfall-iot-regulations.html
- https://www.etsi.org/technologies/consumer-iot-security
- https://automotiveisac.com/best-practices/
- http://www.imdrf.org/consultations/consultations.asp

4. Main Risk Areas

- OWASP's top 10 list of IoT vulnerabilities | Device Authority
- NIST Cybersecurity for IoT Program
- FIPS, Advanced Encryption Standard
- Report: healthcare IoT, Devices most impacted by TCP/IP vulnerabilities (HealthITSecurity.com)
- IETF, best current practices for securing Internet of Things (IoT) devices
- https://www.ssi.gouv.fr/guide/recommandations-relatives-a-la-securite-des-systemes-dobjets-connectes/ (document in French)
- NVD - CVE-2021-44228 (nist.gov)
- Apache Log4j Vulnerability Guidance | CISA
- What the Log4j vulnerability is, who is affected - NCSC.GOV.UK

5. Risk Management and Capital

- https://www.cpomagazine.com/cyber-security/iot-based-ddos-attacks-are-growing-and-making-use-of-common-vulnerabilities/" \t "_blank
- https://threatpost.com/top-10-iot-disasters-of-2019/151235/
- https://firedome.io/blog/top-10-iot-cyber-stories-of-q1-2020/

Glossary

Abbreviation	Description
RFID	Radio Frequency Identification
ENISA	European Network and Information Security Agency
IEEE	Institute of Electrical and Electronics Engineers
ITU	International Telecommunications Union
IETF	Internet Engineering Task Force
NIST	US National Institute of Standards and Technology
IERC	IoT European Research Cluster
IoT	Internet of Things
IC chips	Integrated circuit chips
REE	Rare Earth Elements
IIoT	Industrial Internet of Things
CAGR	Compound Annual Growth Rate
B2B	Business to Business
B2B2C	Business to Business to Consumer
GDPR	General Data Protection Regulation
DORA	Digital Operational Resilience Act
ETSI	European Telecommunications Standards Institute
ESO	European Standards Organization
ENs	European Standards
CSA	Cloud Security Alliance
EIOPA	European Insurance and Occupational Pensions Authority
PAYD	Pay As You Drive
ESG	Environmental, Social, and Governance
REOs	Rare Earth Oxides
PCB	Printed Circuit Board
MGA	Managing General Agent
ORSA	Own Risk and Solvency Assessment

Disclaimer

The CRO Forum is supported by a Secretariat that is run by KPMG Advisory N.V.
Laan van Langerhuize 1, 1186 DS Amstelveen, or
PO Box 74500, 1070 DB Amsterdam
The Netherlands

www.thecroforum.org

cro forum