INTERNATIONAL INSURANCE SOCIETY

An affiliate of The Institutes | Risk and Insurance Knowledge Group

Internet of Things Insurance Gateway

Synopsis

The Internet of Things (IoT) has been developing over the last 20 years and is often referred to as Industry 4.0 or the “fourth industrial revolution.” It is an umbrella term for all the digital assets and entities connected to the internet.

Many of these are intangibles, such as data, human capital via artificial intelligence (AI), intellectual property (IP), and cyber; as such, they need to be made tangible to address value on a balance sheet. Others are connected entities, such as sensor devices, collecting and receiving information in an intelligent fashion across networks.

In time, the term IoT will disappear, as an embedded form will emerge where all the entities merge into a global ecosystem. This will include broad insurance innovation based on device-to-device interaction—something that is already apparent in autonomous transport.

The insurance industry could foresee conservatively as much as $1 trillion in new premium should it address the risk management correctly in terms of data/cyber integrity, multicloud computing, and cyber risk mitigation strategies, plus adoption of regulation and rating around all internet-based network connections. The article on data integrity recently published at the IIS[i] is a foundation to this type of risk management, raising the bar by treating data as a valued asset and moving the chain of truth below based on trust and verify.

The COVID-19 pandemic has increased and accelerated multicloud adoption and digital transformation across all business sectors. This, in turn, has increased cyber threats such as ransomware and exploited weak spots in software supply chains, both of which were very visible at the end of 2020.

This paper looks at how organizations can get visibility into all their different cloud environments and IoT networks to know which cloud they are in, what assets they need to protect, what actors (devices or people) are doing what, and how data is accessed. Once integrity is established, we discuss creation of an insurance IoT gateway accessible by the insurance industry and its clients.

The term “data access” comes from a legacy world where data had to be physically shared to make use of it. We introduce the concept of “data visibility,” where data does not travel and is analysed in situ, at the place of origination, with a secure cryptographic seal around the data and existence of a data provenance audit trail marking nonrepudiation. This satisfies cross-border data privacy laws. When data has to be moved, as in making payments, we can manage seamless transfer of data, without compromise, based on event triggers—often referred to as “data liquidity.”

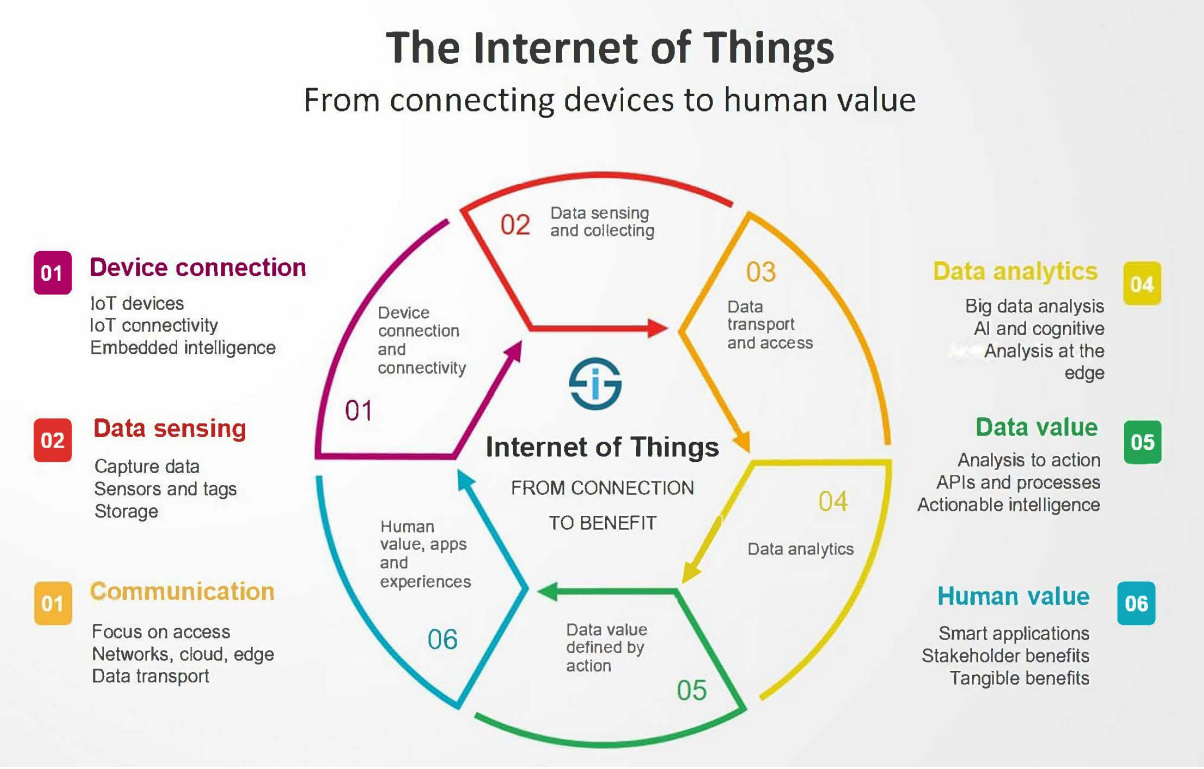
Overview

IoT extends the power of the internet beyond computers and smartphones to commercial and consumer process environments.

Over 20 years ago, Sun Microsystems founder Scott McNealy said, "The network is the computer," which exposed the first green shoot. He also said that “by 2020, all things will be connected to the internet.” His vision was sound, but he could not have predicted the pandemic that has now accelerated an already active IoT development.

Many machines now talk to other machines, with computing being distributed across diverse networks. IoT is a simple concept, taking all the things in the world (people and devices) and connecting them to the internet.

When something is connected to the internet, it means that information can be sent or received in a smart manner. With cyber ransomware attacks rising exponentially during the pandemic, the bar needs to be raised in cybersecurity, which is turn creates an opportunity for the insurance sector. According to International Data Corporation (IDC), there will be 25 billion connected devices in the IoT in 2021, growing to about 75 billion by the end of 2025[ii] The following diagram is frequently used to show the IoT and succinctly captures its key principles.



Worldwide spending on IoT is forecast to pass $1.0T in 2022, reaching $1.1T in 2023, with a market opportunity of $4T by 2025 spread across industrial and consumer ecosystems. IDC further forecasts that the 75 billion IoT-connected devices will produce data volume of 79.4 zettabytes by 2025.

For insurers, machine-to-machine identity drives device-to-device insurance. The confluence of exponential technologies such as blockchain and AI (machine learning) to IoT opens up endless possibilities. The emergence of very low-cost computers (such as Raspberry PI), [iii] which can be plugged into the network through any device, brings in global communities as citizen developers. Commercial solutions of smart transport, smart cities, robotics, manufacturing, healthcare, energy utilities, and more are already in place with the 20 billion devices linked to the internet today. Digital, autonomous agents interact with devices and

connect them to networks, platforms, and gateways that exist in cloud-computing environments. These agents feed each other to democratise IoT data, transacting in a real-time manner with identities like people.

It is in the interaction of these digital agents where new insurance strategies can be embedded in the ecosystem to collect premium and pay claims in a parametric fashion using trusted granular data as triggers coupled with predicted analytics. Technology, conversely, will gradually reduce premium from traditional insurance as is happening in the motor sector as risk-pooling changes to individual insurance based on pay-as-you-drive. Therefore, it behoves the insurance community as a protection industry to replace that lost premium and create new insurance markets while at the same time shortening tail of risk to benefits of the customers with data privacy, data governance, and faster claim paying.

Cross-border issues can lead to arbitrage digital frameworks, so there needs to be regulation and standards involved. Governments and regulators have key roles to play in managing the multicloud environment that requires open common standards across borders with a decentralised environment of shared value. This creates a need to measure data and ownership on devices to determine who shared the data; who uses it; and most importantly, who is liable in event of a breach—reflecting a tectonic change from the internet age into an era of transformational technology based on truth leading to data sovereignty, where data has a true tangible value that can be shared with insurance companies with permission and premium discounts.

In effect, the internet is wrapped with what is essentially a lie detector for data based on blockchain technology. The emergence of regulatory technology (regtech) and regulatory sandboxes will counter the fact that no technology is neutral, so bias is mitigated. The onus is on society not to create another period of digital divide.

Privacy must be preserved and include a legal framework around cryptocurrency developments for reserving and solvency calculations. The digital wallet becomes the new firewall cryptographically sealed, and data now becomes the perimeter enabled by blockchain technology as the control layer for data integrity in the cloud environment.

This paper looks at the importance of cloud cybersecurity and how IoT can become a new market for insurance, increasing premiums and country GDP, keeping insurance relevant in the digital era as a key protection strategy. However, there have been interoperability challenges of execution platforms in IoT manufacturing sectors, signifying the harbinger of change. Better connections and a lower carbon footprint of sensors in line with ESG expectations by energy harvesting extend the life of sensors.

The COVID pandemic has highlighted the need for data and cyber integrity by requiring monitoring and coordination of data visibility across holistic supply chain processes. Post-pandemic IoT will reveal a more operationally efficient, green-based technology with data tamper mitigation.

IoT Security, Regulation, and Rating

The IoT is umbilically connected to the cloud. The world is moving to multicloud environments at an accelerated rate, fueled by the pandemic and climate change, as moving away from corporate data centres improves carbon footprints.

Security in the cloud has greatly improved, but billions of interacting devices communicating and learning from each other with AI brings new challenges for cybersecurity, as

organizations need to consider what is happening beyond their network. With the increase in ransomware attacks going up 25 times in 2020,[iv] cyber integrity is paramount.

Geopolitical tensions and data-localization laws also demand cross border standards for data and networks. And the increase in connected solutions attracts attackers looking to steal personal data or take control of devices for various purposes. The challenge is to make sure devices are adequately secured—and currently there are weaknesses in how manufacturers leverage security.

Concerns have been voiced over lack of security in many IoT devices, so now industry trade groups are looking at security ratings for these devices[v]. Vulnerabilities exist in devices from manufacturing, and no one knows what is in the component black box anymore. Because wireless components are distributed across networks, they are most vulnerable.

Many vulnerabilities are caused by protocol-level flaws that can be addressed by online regulatory compliance (discussed later as a key mitigator for insurance). For example, old operating systems devices may not be able to be patched. This has been a chronic problem in healthcare, as many hospitals do not test their medical devices in the IT domain and lack the protection against zero-day breach and ransomware.

At the time of this research, Australia and the UK lead the charge on IoT security. But in 2021, several states in the U.S., including California, will enact legislation. The ratings will be assigned to the devices at OEM (original equipment manufacturer) or manufacture time and data integrity proof is a key rating item on the data that the device receives or sends, and this will be a key underwriting parameter. Regulators do not want consumers to become complacent on security because a device has a high rating. Sensors must be revaluated on a regular basis because of the exponential pace of this trend.

There are differences in the traditional preecosystem insurance world, where rated burglar alarms were used as standards in policy wordings, but in IoT, a device interacts with a host of other devices, so the cybersecurity of the connectivity has to be taken into consideration.

The insurance industry needs to mitigate against systemic risk, which is heightened in such an ecosystem. This has to be in tandem with governments designating certain cloud environments as critical infrastructure around defence, energy, and utilities, which could lead to serious disruption and loss of life if breached.

However, not all data breaches are caused by bad actors, and the effects of accidental misconfiguration internally or disruption by increasing natural disasters has to be realised. A high percentage of data breaches are accidental and can be prevented in line with the mitigation of deliberate and malicious attacks, so implementing data integrity while preserving privacy is the siren call here. The EU, U.S., and Australia have put out serious data breach notification laws with harsh penalties. In February 2021, Singapore enacted a similar act, forcing data integrity mitigation and prevention, and China will follow. This includes cascading destabilizing effects on business interruption for clients, the economy, and society, coupled with the cost of social inflation.

Insurance is secondary risk transfer to this mitigation, and regulations also apply to offset physical or financial damages resulting from cloud-computing failures. Current insurance policies are not sufficient to cover the accumulation risk, with only modest amounts covering breach reporting and legal expenses. At present, insufficient insurance recourse is available to cloud service providers or policyholders to address this scenario. Detractors will say that

this is not an insurable risk, as it could be equated in the same category of mass internet failure.

The nascent cloud insurance market does not currently offer extensive solutions because of systemic risk that accumulates as a result of the cloud's market concentration cascade risk. System failures potentially affect many different parties simultaneously, trickling upward, downward, and sideways, and resulting in a mass of claims that could prove excessive for insurers and reinsurers to cover. Regulators' concerns over the solvency of (re)insurers that underwrite cloud services in these domains are bound to further slow expansion of insurance for cloud service business interruptions, especially as they pertain to coverage of damages to third parties.

A phishing attack on a connected corporate device, such as a smartphone, can cause several IoT sensors to be infected with malware and disrupt a manufacturing plant's production line. Organisations can no longer consider cybersecurity risk solely in the context of their particular backyard, as the IoT is an ecosystem with platforms and services shared by different application domains.

This brings a new dimension to cybersecurity. The solution is to add cryptography and AI to the devices and data for awareness and to search for real-time vulnerabilities, such as those deployed in the government of Estonia, NATO, and the defence industry.[vi]

Confluence of Cloud Computing and IoT

Cloud means "somebody else's computer." This simple truth is the root of the data sovereignty, security, and trust problems that have hampered cloud's adoption by the public sector and in critical regulated sectors.

Cloud is not a new idea but is only now fully coming into its own. It provides the infrastructure for processing big data, providing customer-friendly services, and adopting new technologies (such as AI, 5G, and edge computing). But cloud is also a major business process innovation where companies can outsource their entire IT infrastructure, bringing in new competence in everything from accounting to customer service through software-as-a-service, and then focus on their core business. This allows small organizations to scale up operations quickly, while big organizations that embrace cloud are leaving their competitors behind.

Among Fortune 500 companies, cloud adoption is near universal. However, European companies lag their American competitors, with SMEs (small and medium enterprises) faring worst, with Asia leapfrogging due to less legacy encumbrances. Despite European and national cloud strategies, a similar gap can be seen in the public sector, with little European government uptake of cloud services.

Concerns over security and governance have been a serious impediment to cloud uptake. These concerns have been exacerbated in recent years by questions of digital sovereignty and data protection (for example, through the EU General Data Protection Regulation). To get the true benefits of IoT with the right level of security, data integrity and privacy organisations need to move to ambitious cloud posture to leverage public/private/hybrid multicloud strategies and stay relevant.

On the commercial side, there is a conflict that needs to dovetail for IoT to function. Information technology (IT) and operational technology (OT) are very different, as the former is based on data processing and the latter on engineering. Because of digital developments,

they are now working in confluence which could be a dangerous risk exposure for critical infrastructure and the lives of the people that operate them. OT on factory floors or railways tends to only look at physical security; that is too much exposure, as most of the serious breach wake-up calls have been data-integrity motivated.

Cloud computing itself is morphing and endorsing edge computing, a vital component of IoT networks, where the originating data is processed by the device itself or by local computers rather than being transmitted to a cloud data centre. If we think of the modern car as another device on the network, we can easily understand the autonomous car in this regard.

For the insurance industry to understand the implications of IoT for risk and opportunities with emerging cloud technologies such as edge, in conjunction with AI and 5G connectivity, it must first be aware that it no longer needs to access the internet directly to function. An example is a hotel lighting system controlled in the cloud. Should there be a glitch with the internet connection at the time the hotel network switched the lights on, there is a risk that the lights would fail. However, if the cloud itself were the hotel network, then there would be no need to access the internet.

Another example is an autonomous car. If the braking system required a call to the internet, disaster could result. So, the cloud must be the car itself.

For data integrity, creating data provenance to the nearest point of origin is a KPI (key performance indicator). So edge computing means the data does not have to be moved but has visibility and can be shared and analysed in real time with permission in situ. If required, data can still be transferred to the central cloud for more sophisticated processing of data at scale.

The power of AI at the edge becomes obvious as machine learning is embedded in sensors where data is being collected to mitigate and make life-saving decisions in healthcare (e.g., pacemakers), smart city grids, or production issues in manufacturing. This means moving software code to data collected at the edge of the network so that it is processed and analysed in real time, allowing knowledge to be transferred in places where split seconds matter. These are local triggers that become tags for parametric insurance design at endpoints in a network.

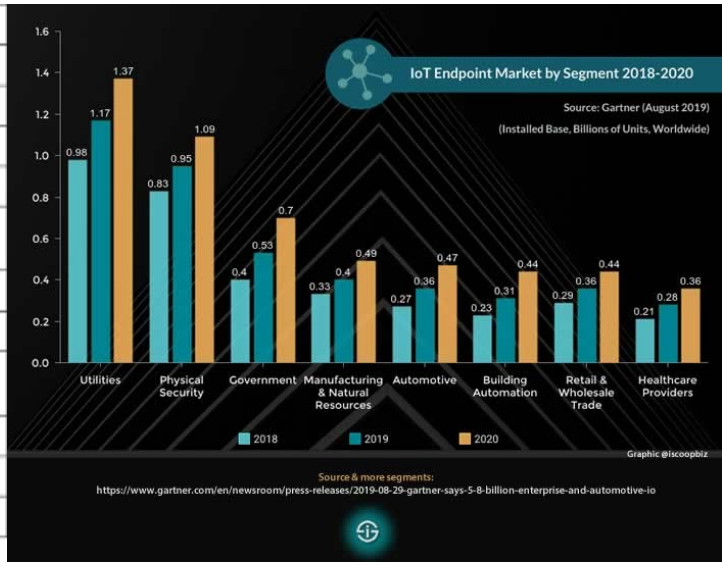
Anything that is attached as an endpoint to the internet and can sense and send data is part of the IoT. An endpoint is what makes an object uniquely identifiable. It can be (part of) a system, device, tag attached to an animal, or sensor and communication system connected to a human being.

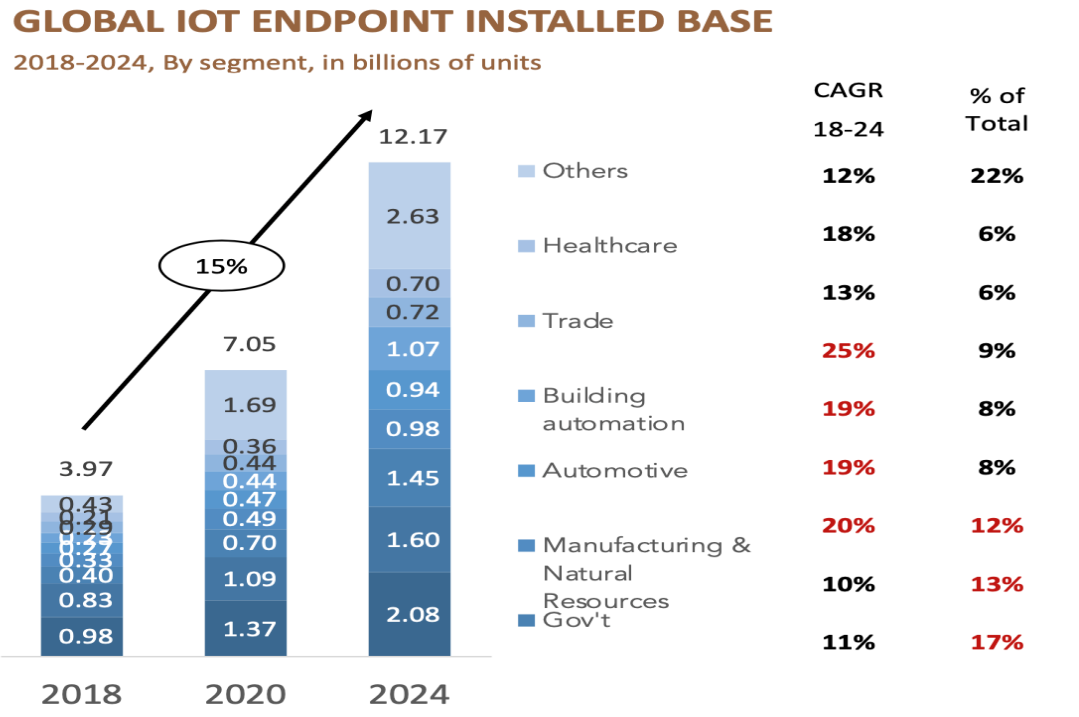
Connecting all these endpoints to the internet requires an Internet Protocol address (IP). The newest version of the protocol IPv6 allows for an almost infinite number of IP addresses for the IoT networks to consume as the service-based economy manifests itself in the mainstream with process automation and data analytics. The endpoint security market is expected to reach $18.6 billion by 2027[vii], growing at a compound annual growth rate (CAGR) of 5.9% during the forecast period of 2020 to 2027.

The 5G endpoints are physical computing devices that provide faster connectivity with lower power and latency. These results are expected to achieve large CAGR growth as 5G cellular networks take hold globally. The following charts show the current and future endpoint growth by sector.

Segment	2018	2019	2020
Utilities	0.98	1.17	1.37
Government	0.40	0.53	0.70
Building Automation	0.23	0.31	0.44
Physical Security	0.83	0.95	1.09
Manufacturing & Natural Resources	0.33	0.40	0.49
Automotive	0.27	0.36	0.47
Healthcare Providers	0.21	0.28	0.36
Retail & Wholesale Trade	0.29	0.36	0.44
Information	0.37	0.37	0.37
Transportation	0.06	0.07	0.08
Total	**3.96**	**4.81**	**5.81**

Source: Gartner (August 2019)





Insurance and IoT

The opportunity within the insurance industry is an IoT protection gap, or the amount of new insurance premium that could be generated from protection products on IoT, which is currently not being addressed. Seventy-five billion devices are predicted to be online within the next decade, generating 10 terabytes of data per second. These new products will be able to collect instant premium based on parameters or conditions (smart contracts) via sensors. In return, automatic pay out of claims will be expected when a predefined condition is achieved.

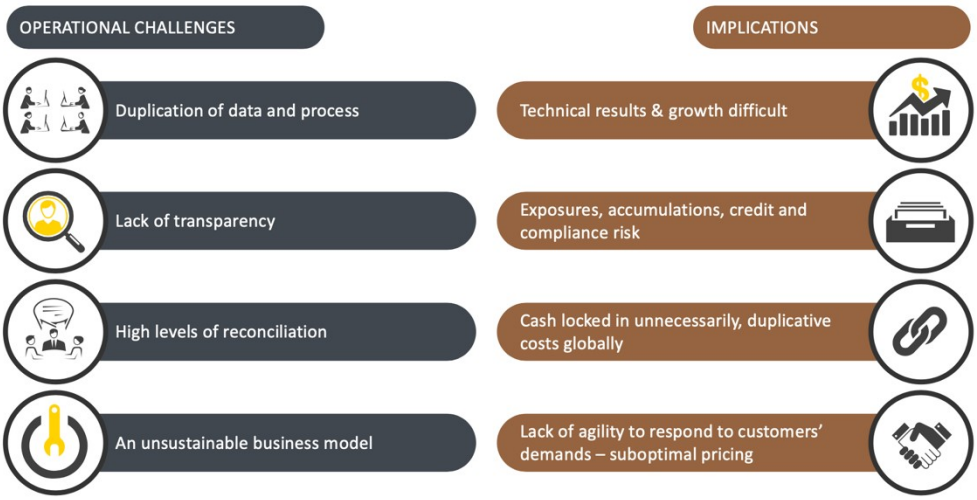
This gives rise to parametric-based insurance where alternate means of insurance and reinsurance are deployed to cover new risks and exposures. With the expansion of IoT, this will undoubtedly be the future of insurance, as protection cover becomes embedded in devices (both commercial and personal). This approach will address several pain points extant today—namely, reduction of digital fraud; faster claims paying; lower expense ratios; and more accurate identification of liability in a multiparty, multilocation situation once data integrity is mitigated. The implications for the P&C and healthcare insurance sectors are self-evident, but for the life insurance industry, changes will be more subtle.

As an agent-dominated domain, the life sector has seen a slower transformation since the emergence of digital life insurers. In similar fashion to the pay how you drive (PHYD) in the motor sector, the life industry enters a pay as you live (PAYL) era, where IoT networks can be leveraged as new distribution channels and OEM partnerships can be stablished with device manufacturers and insurers. This will bring IoT-related service and business models to the table, especially to the sustainability of the aging society and retirement products. Risk assessments will move to a data-driven approach and distribution will shift to online delivery as the life sector aligns with the rest of the industry transformation, with faster paying of death claims an immediate priority.

IoT Insurance Gateway

In order to create an effective insurance offering from IoT, there is a need to first create a single picture across the enterprise by monitoring digital assets in real time and to bring all multicloud components into a single pane of glass. Because of the size and extent of IoT, real time forensic immutable evidence is required to seal proof of time the data was created, the identity of that data, and whether there is any data tampering from the original state. This is situational awareness of all the important assets in an enterprise and can stand up in a court of law.

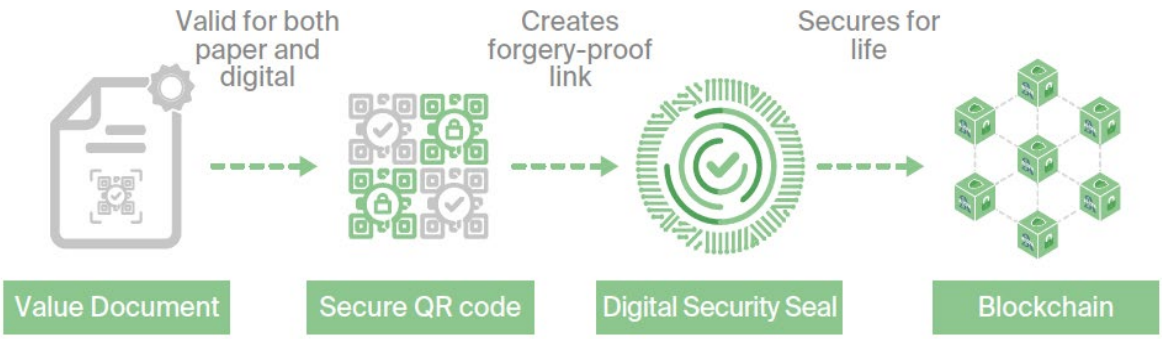
IoT gateways are assets that enable data to be analysed at the edge of the cloud at origin. We have extended the concept here to allow access to an insurance gateway for use to create insurance products using data-driven underwriting. The diagram below shows current challenges in the status quo that are being addressed.



By enabling data to move from IOT devices, machines and vessels in real-time and with cryptographic guarantees, processes can be automated creating a market place for risk based on asset behavior instead of historical data.

The question to be asked is, How do we make sure that the resulting IoT insurance marketplace does not contain false data and identities?, as it will be driving underwriting and triggering claims and interoperating with placement platforms. This holds true whatever sector we are addressing. Substandard or counterfeit products entering a supply chain will affect all the insurance touchpoints. So underwriters need to understand the concept of digital physical twin technology[viii] if they are to drive new business outcomes from IoT.

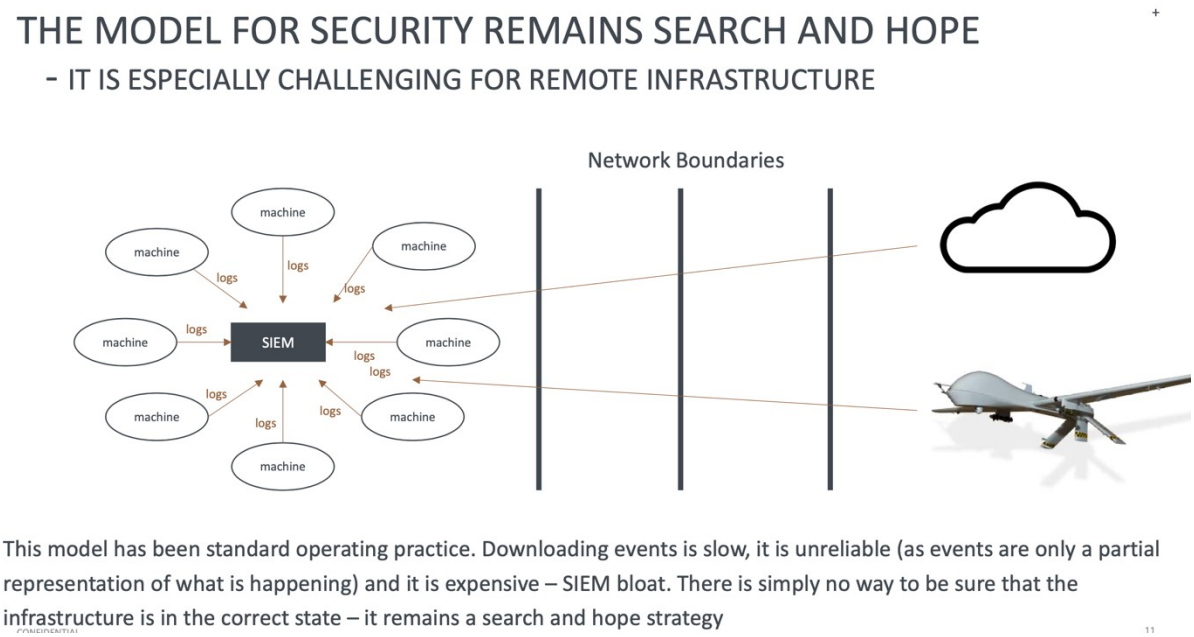
The premise is, that in such an ecosystem, there should be a digital cryptographic representation of every physical asset in order to verify the veracity of that entity. This gives security and trust that any physical asset or product with a digital twin can be monitored in real time and is in fact authentic throughout the lifetime of the asset. A blockchain-based system can be fooled by the entry of a substandard physical entity, such as counterfeit drugs or lithium batteries, which can lead to loss of life. The only way to counteract this is to secure identity to a digital twin with cryptographic integrity. The diagram below shows an example of such a link.



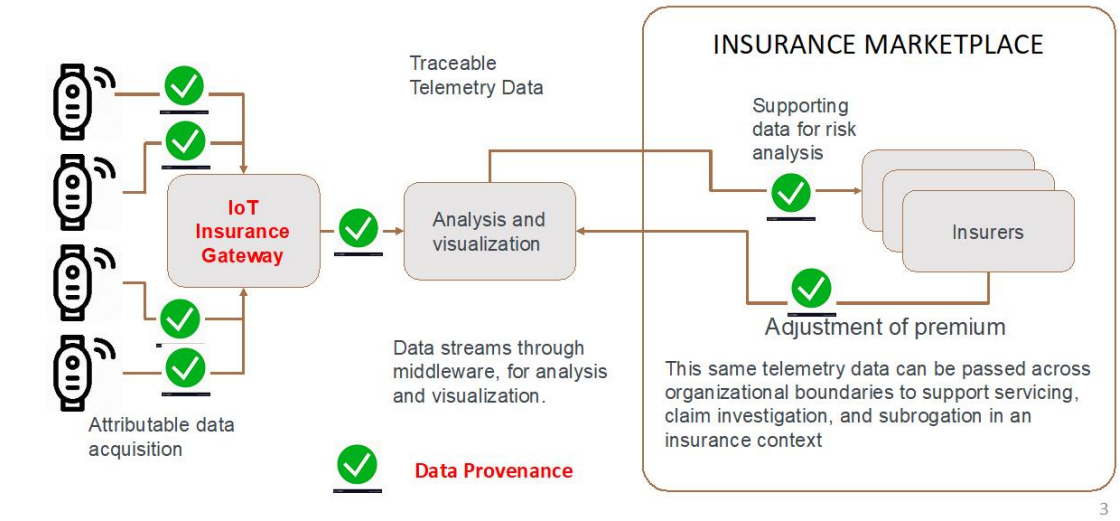
This process ensures that every digital asset on the network is assigned an immutable digital physical twin, which connects the physical and digital worlds by taking real-time snapshots that capture the reality of the target infrastructure. This immutable forensic evidence acting as an independent witness can be utilised by third parties, such as regulators, auditors, and insurance companies. This can prevent configuration mistakes and roll them back before they are applied.

Established security standards (such as from NIST or ISO)[ix] or insurance regulations are built in to ensure compliance and reporting. Having this predictive data reduces the need for modelling and costs from the bug bounty programs, where millions are paid to white hat hackers and vulnerability research to find flaws. The IoT can help by making use data to increase transparency and predictability of such processes, understand the limitations of computational modelling and techniques, and improve the assumptions that these models are based on, thereby reducing overreliance on modelling.

The constant inspection of granular IoT data and the possibility of sharing aggregates to increase transparency between parties can help insurers and reinsurers to understand strict liability and its sharing across parties across complex ecosystems. Recent breakthroughs in machine state integrity at Verizon[x] have enabled security professionals to advance beyond the limitations of handling networks, as shown in the diagram below, to allow a new frontier that is achievable now.



This represents the opportunity for insurers to act on the right kind of data at the right time, leading to improved coverage and liability of nontangible digital assets while still mitigating the dynamic nature of cyber risk. IoT counters the argument that there is not enough data to understand the risk to address adverse selection and moral hazard concerns. The following diagram shows the flow of attributable data into a new marketplace:



Most importantly, this works with edge computing as described earlier where a majority of IoT happens. The global edge computing market is expected to reach $6.72 billion by 2022, at a CAGR of 35.4%[xi]. Any change in the environment out of policy generates a high-quality alert that can be remediated in real time. The measurable value to insurance will be that insurers understand the risks better, especially around behavioural pricing of risk.

Provable compliance means that customers are not accidentally at risk due to error. Opening the door to a new era of parametric insurance, provable compliance will allow clients to receive faster claim payments with less subrogation and fewer disputes. Discounts and rebates can be given for proper maintenance and good safety practices. Pay as you go insurance products, which are priced in real time, based on trusted granular data, can be offered. The technology is here, and insurtech companies or legacy insurers adapting to insurtech's are in a position to take this up in 2021 and beyond.

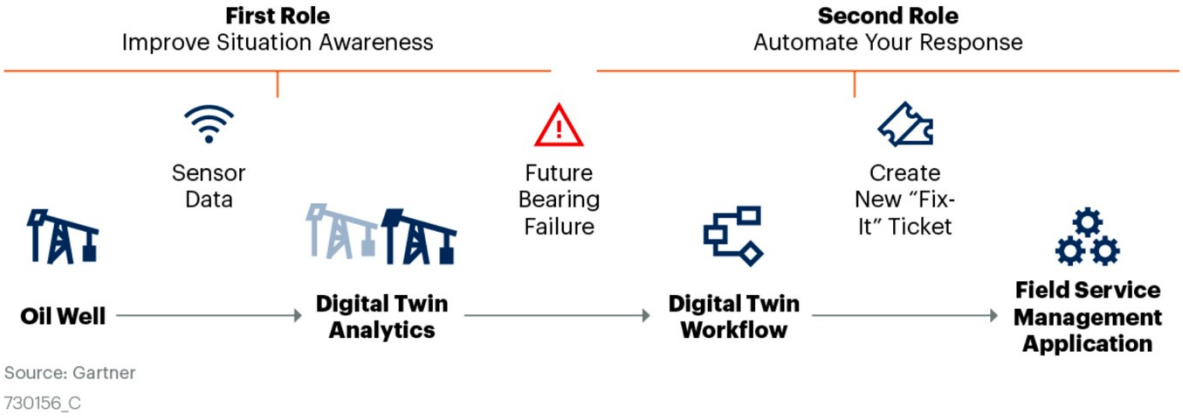
New ecosystems can be created where connected device usage by affinity groups can lead to new applications and forms of community ecosystems, such as mutual insurance peer–to-peer communication with each other and through gateways, connected to an IoT platform where the various applications of the organizations are ingested and triggered. These platforms are often supplied by big cloud providers, such as Amazon and Microsoft. Faster 5G networks will support virtual reality data streams which will be built into autonomous transports, factories, utilities, and smart ports and cities.

Payment Systems

If we are to pay claims and collect premiums from devices, the Internet of Payments needs to evolve in parallel. It is necessary to have seamless and instant access to payment services from each endpoint in the network, via a digital interface. Identify and KYC (know your customer) largely through biometrics is paramount and controlled by blockchain technology and encouraged by regulation. This means anything IoT connected can make a payment by triggers attached to e-wallets, which can be licenced for collection by insurers

and prefunded for claims. Smart contracts will play a big role here, with blockchain enabling the provenance of the payment process.

Data and cyber integrity is about creating situational awareness of every piece of data in the network so as to render it tamper free and render provenance to the original. Here is an example of making a payment to a vendor from an endpoint in the commercial network: The oil well detects a fault that needs correction before failure occurs and generates a maintenance ticket, which is paid and enters the accounting system.



Legacy Systems and the IoT

Legacy systems developed in the pre-IoT world are numerous and need to be included in IoT-integration strategies even though they are not compatible. However, they will not survive as the networks speed up.

IoT development will be the biggest driver for retiring these legacy systems. This can start with lifting and shifting systems to the cloud and then splitting out the legacy into microservices, each with its own secure API (application programming interface). This is a move to a software–as-a-service operation to be able to operate in an ecosystem. Adding machine learning or AI to the API further enhances the process.

Legacy systems in general do not have the ability to keep pace and scale with digital transformation and are not designed to operate at the edge of the cloud. However, because of investment, especially in manufacturing systems, factory owners are retrofitting IoT sensors to their legacy systems. This brings cybersecurity concerns to the table, as privacy and security, by design, were not original features.

Every industry has a life cycle of its assets—and this cycle can be long (for example, 30 years in cases of factory hardware and long-running life insurance policies). This means there is a lot of legacy to deal with in all sectors, and rip and replace is not an option for boardroom investments that are still fit for purpose. However, over time, they will not survive the technology changes, so companies need to start planning legacy transformation. In the meantime, the cyber strategies mentioned in this paper also apply to legacy, so we need to make sure there is no exposure. A lot of the digital transformation for legacy will come from open source developments, so it is important for security that the real-time snapshots of the enterprise network include the API and microservices (breaking out legacy into mobile apps) in an integration strategy.

Data Valuation and Ownership

Looking at a world where there is continuous connectivity with data sharing brings up new conundrums on how we look at liability. A common catchphrase now is, “Data is the new oil.” This presupposes that data is a tangible asset, opening up scenarios about, for example, who owns the data on a device and who has product liability when a connected car crashes. A real and far-reaching opportunity is to assess how data, an intangible, can be valued as an asset and assessed by organizations, as well as how these advances in data integrity pave the way for this development. Once it is tangible on a balance sheet, data can be mathematically modelled along with other assets and offset against liabilities—and that future value can be traded on a data exchange.

Governments need to recognise the value of tangible data so they can give corporate enterprises the freedom to operate in economies in exchange for de-risking their activities. This allows for a prenegotiated free passage of the open and unique development of new markets.

It follows that this recognition and valuation would need to be supported in government tax schemes. Intangibles are worth more than tangibles, and when combined, are difficult to imitate, thus leading to competitive advantage. It follows then that, by estimating the value of data, executives can manage organizational competitive position much more easily. The value of the data can be embedded in the strategy of the organization by closely aligning its measurement with company strategy. This leaves us to see how we can protect data integrity so that we know that the data is tamper free and intact. With that warranty in place, the valuation of data becomes a quantitative practice so that new ideas and innovation will become mainstream activity.

The IFRS (International Financial Reporting Standards)[xii] outlines the recognition and measurement of intangible assets. It is not a straightforward practice to value data and must be linked to an integrated reporting and accounting framework and then holistically correlated with other risks, which can inflate or deflate valuation of the data.

Regulatory and legal constraints always apply in different jurisdictions, and data crosses borders, so we need to have the data integrity status on all pieces of data wherever they travel. This is not only the data itself, but the metadata that defines it. Governments, sponsors, and investors in new enterprises or new economies may not recognize the importance of an enterprise because they are not informed of the size and value of the data asset. As data increases exponentially, we risk losing sight of where data ownership resides. We have already seen the conflict where data could be unwittingly owned by social media sites because they are smarter at analysing big data. This is likely unacceptable to governments, corporations, and individuals alike, who look to blockchain as a democratizing panacea to this issue.

How can data be valued? The current way is to buy and sell data so it has a value on the market. Without integrity proof, the trust of buying and selling data is diminished.

Another way is to make data part of a macroeconomics exercise, such as a data index in an economic scenario generator, where it is valued to the level of the profits and earnings in the model. It would act as a data exchange where the data asset can be simulated ahead of time for its value, the same way as equities and bonds. We could also tie data to the IoT rating so that data coming from nonrated devices would get a downgrade.

When data is a tangible, it potentially becomes taxable against its value. If data were taxable, then the practice of hanging onto data may decrease and have far-reaching implications for data privacy and ownership.

In conclusion, the data that is input is going to be the output that determines the decisions of the company on a dynamic ongoing basis and is tied to accounting, regulatory, and legal constraints directly affecting the solvency of the business. In the short term, it is more likely that IP and AI algorithms will be valued as tangible assets and precede the inevitable data valuation.

ESG Implications of IoT

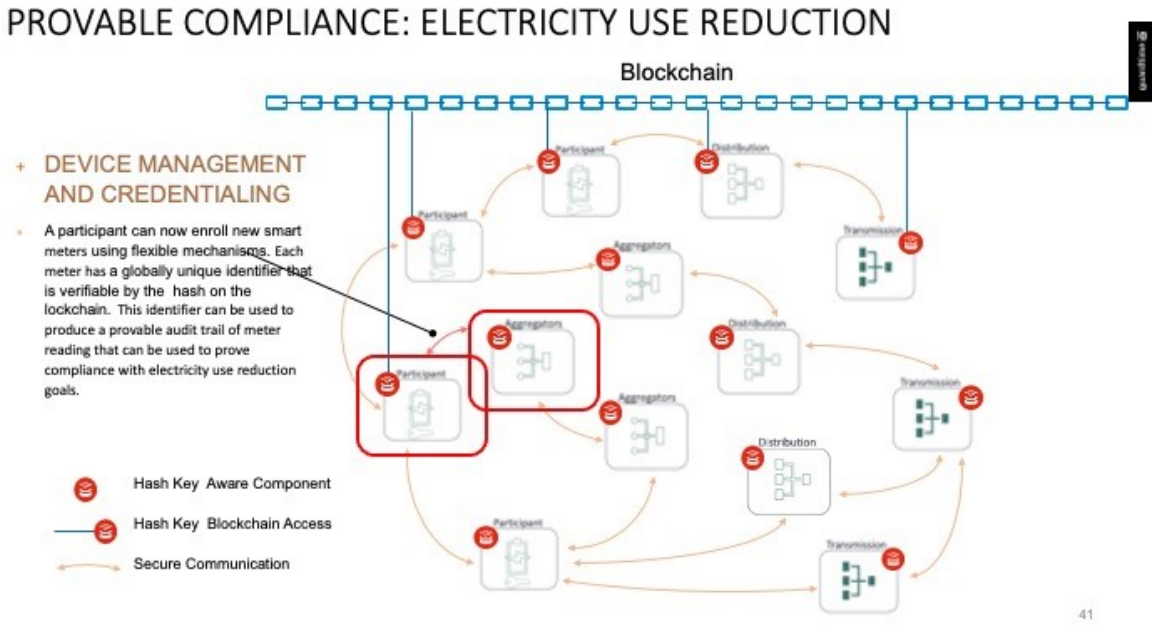
The importance of using ESG (Environmental, Social and Governance) as a risk mitigation tool and long-term investment for the insurance industry is clear. This approach is intended to create a holistic view of all new, emerging and existing risk such as cyber, pandemic, and climate change and then place them into a risk-adjusted framework where correlations can be achieved between defining events and asset portfolios. This is the approach to decarbonize the economy to net zero emissions in the future.

Millennials will want to see the industry create products around climate change mitigation, such as with-profits life policies, only utilising an ESG investment portfolio. In addition, these ESG risk mitigation strategies should line up with the United Nations Sustainability Development goals (UN SDG)[xiii].

The International Insurance Society (IIS)[xiv], the Insurance Development Forum (IDF),[xv] and the United Nations Principles of Sustainable Insurance (UNEP-FI)[xvi] combined forces several years ago to pave the way for sustainable insurance. An ESG rating added to each device at manufacture will give further truth-based parameters along with security for the insurance industry to create solutions.

IoT connectivity will play a big role in climate change risk, energy, and carbon footprint reductions, as sensors measure in real time scenarios not possible before. An example might be around temperatures across supply chains—data that could be stored in a blockchain for analysis by third parties as in the insurance gateway alluded to earlier in the paper. This will drive a change in consumer attitude to choose sustainability over brand and force manufacturers down this path to keep brand reputation.

According to the World Economic Forum,[xvii] over three-quarters of the current IoT deployments address the UN SDG's. The diagram below, courtesy of Guardtime,[xviii] shows how IoT smart meter networks can assist in electricity reduction.



Conclusions

We have established that the Internet of Things, or IoT, is about extending the power of the internet beyond computers and smartphones to a whole range of other things, processes, and environments that will gather and analyse data at speed closely to where the data is originated. This is one of the most important trends of our time, as it is at the very core of the Fourth Industrial Revolution, brought about by exponential technologies. It is significant because it provides both organisations and consumers access to environments beyond the reach of the current internet to make the world more connected and productive.

There are many new businesses now based on service, such as Uber and Tesla, and emerging risks are flipping the insurance world to intangible cover. Motor insurance is the first to be affected by this, as it is a large part of the industry's overall premium. With Uber-type services, self-driving vehicles, pay how you drive insurance, and electric cars, the shift in customer behaviour will reduce that motor premium significantly, leaving a protection gap that the industry has to develop through the process of the car, rather than the car or driver itself (i.e., using sensors and the data from them to form new insurance covers based on process). This has been accelerated by the pandemic which is why the market cap of InsurTech sector and the investments for that sector have now exceeded $100 Bill as they address new processes.

We have set out to prove that the new world order is made of intangibles and that data is the next big thing in the intangible space, serving as the glue that links other intangibles together. It is paramount that boardroom thinking and accounting practices align to this new world structure; otherwise, the lack of ownership of the data and the risk of losing that data packaged up as some form of tradable asset without control could lead to a serious bubble, where data is managed by the wrong people for negative effect.

Companies need to have self-assessment mechanisms to value data and provide a dashboard of the risks and tolerances of the data. Such dashboards can then be reviewed by independent regulators who will drill down to the data component within the operational risk strategy. As of today, operational risk is not well-defined or quantified and is subject to a lot of guesswork.

In conclusion, the internet was created based on trust, not truth. Security issues came later as the technology matured. Digital ecosystems will be the new norm, and companies ignore this at their peril, as they could become digital pariahs.

Young people will share their data, do peer-to-peer evaluations over the digital network, and avoid digital ghettos caused by nonsharing. Within digital ecosystems come the concepts of data ecologies and trusted security services. Herein lies the future, with sensor- and machine-driven authentication, digital identification, data asset exchanges, and digital currencies linked to personal data. This all gives birth to a “digital futurescape,” where personal data becomes the secure guardian of consumer data, digital commerce builds the digital ecosystem, and the result is a secure network of smart and seamless services. The data asset exchanges will aggregate, value, and trade digital assets with transparency and integrity across all sectors of business, government, and universities.

Indeed, we are at a crossroads of titanic exponential change in both the commercial and retail worlds, especially for insurance, as it is rules driven. However, the mathematics of insurance does not change because of digital transformation, as the industry in most part obeys the laws of physics by correlating chains of events based on scientific laws using high order mathematics. This will be paramount for risk management in the IoT arena.

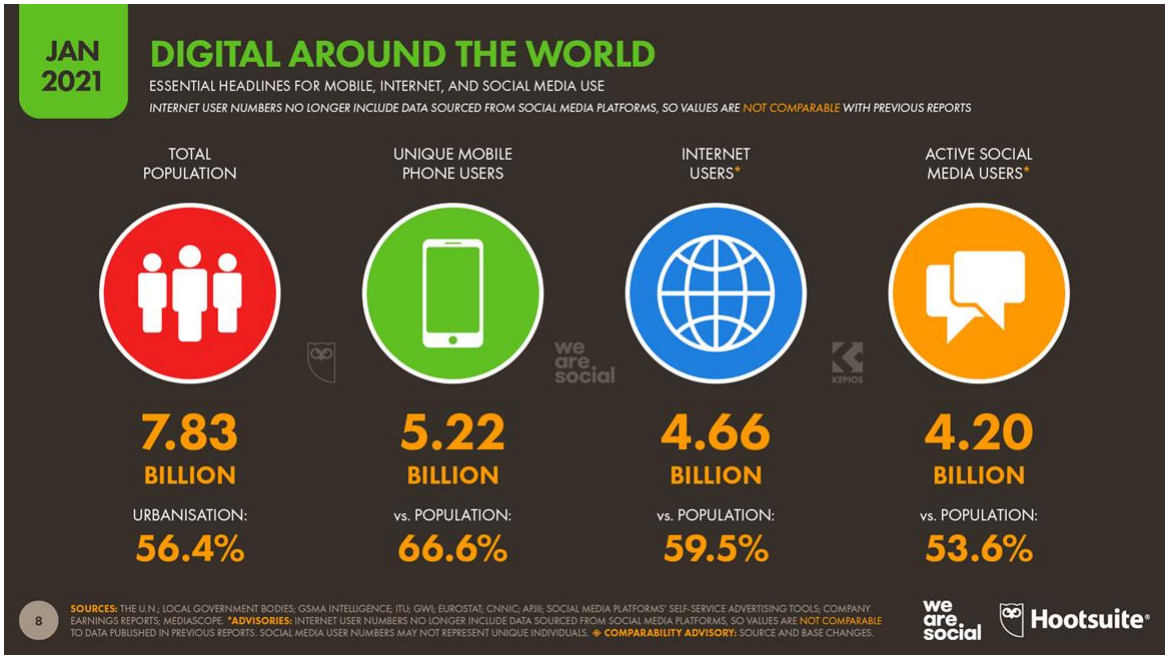
Future Considerations

The future, in summary, is digital first and cloud first for the consumers. The cloud will move to edge computing. Because of the vast increase in devices/endpoints, data, and 5G networks, we expect to see faster and greener technologies coming in a matter of dog years. These technologies are around a different way of computing and embedding AI and sensor capabilities into chips.

Quantum computing and All Photonics Networks (optical fibre) will drive greater speeds at lower cost of electricity and lower latency. Quantum computing renders the current encryption process (PKI) ineffective, so the use of blockchain cryptography is required to render all privacy of IoT digital assets quantum immune.

Currently, a graphics processing unit as used in the gaming industry processes much faster than a central processing unit and allows virtual reality to be applied. Quantum computing has the faster effect and allows AI and machine algorithms to crunch data and do calculations at lightning speed. Widespread use of this technique is just a few years away.

According to Gartner, in 2021, $699 million will be spent on quantum computing by the U.S. government because the amount of AI-generated data in the next few years will overcome the capacity of traditional computing. With new technologies like 5G, a host of cyber vulnerabilities come layered on top, and a lot of investment is required in trend research to find vulnerabilities in these new technologies. The global scene is set as the world becomes digital.



Exponential technologies in combination dictate the future for Industry 4.0 and shape the future of both commercial and consumer insurance. Blockchain is the mechanism by which we achieve trust in ecosystems, preserve privacy, and get data integrity across borders and outside the territory of the internal organization. The blockchain IoT market is predicted to grow 73.5%, to a value of $31.2 billion by 2030.[xix] AI, in conjunction with faster networks and edge computing, is the big game changer for cognitive machine learning and citizen development.

For big data collected, it is likely that AI will address the establishment of small datasets to drive change in the insurance industry for real-time actuarial pricing and data analytics. Digital twin technologies will increase as the agents of change in supply chains and ecosystems. This is the coming of age of tokenisation, in conjunction with security token offerings (STO) and SPACS (special purpose acquisition companies) bringing insurtech into the public offerings. CBDC (central bank digital currencies), where fiat currency is pegged to digital currency, will address and stabilise volatilities in solvency calculations. These developments complete the virtuous cycle of monetising IoT.

These ecosystem developments allow for peer-to-peer interactions and align well with the rise of mutual insurance in the developing world and with Takaful insurance in the Islamic demographic. This is a major game changer for microinsurance and financial inclusion; hence, the investments from World Bank are increasing and encouraging citizens' open source development. Raspberry Pi computers now cost very little, and poor communities in developing worlds can access the IoT with safe transfer of data among parties.

Cybersecurity improvement is a priority for the future. Early IoT arrangements are reliant on a central architecture where data went to the cloud, was analysed, and then returned to the device. With the billions of devices attaching in future years, this approach exposes many endpoints, is not scalable, and jeopardizes network security. Using blockchain, the data is shared over a distributed, cryptographically protected network and analysed in real time at point of origin.

So, for the insurance industry to weigh and insure cyber risks, and back the IoT, evidence of integrity in an organization's data and in information rules governing the systems that

manage that data is necessary—and should be independently verifiable, without having to trust the organization hosting those assets. This baseline instrumentation will allow the insurance industry and the organisations it backs to better identify and visualize threats and changes to important intangible assets.

Fundamentally, integrity instrumentation allows you to tag, track, and locate all the IoT assets in cyberspace for use in next-generation insurance products.

Endnotes

[i] https://www.internationalinsurance.org/index.php/Insights-Cyber-DP-Cyber-Insurance-Integrity

[ii] https://iotbusinessnews.com/2020/08/10/08984-connected-devices-will-generate-79-zettabytes-of-data-by-2025/

[iii] https://www.analyticsinsight.net/raspberry-pi-the-next-revolution-in-the-internet-of-things/

[iv] https://cyberflorida.org/covid/bitfender/

[v] Global industry frameworks and best practices, such as the National Institute of Standards and Technology's Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers (draft NISTIR 8259) "Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline,"; the European Telecommunications Standards Institute's Cyber Security for Consumer Internet of Things (ETSI TS 103 645); and the Council to Secure the Digital Economy's C2 Consensus on IoT Device Baseline Security (CSDE C2 Consensus).

[vi] https://ccdcoe.org/

[vii] https://www.globenewswire.com/news-release/2020/06/14/2047736/0/en/Endpoint-Security-Market-Worth-18-6-Billion-by-2025-Growing-at-a-CAGR-of-5-9-from-2020-Global-Market-Opportunity-Analysis-and-Industry-Forecasts-by-Meticulous-Research.html

[viii] https://www.networkworld.com/article/3280225/what-is-digital-twin-technology-and-why-it-matters.html

[ix] https://www.itgovernanceusa.com/iso27001-and-nist

[x] https://www.globenewswire.com/news-release/2020/09/03/2088529/0/en/Verizon-advances-5G-network-and-cyber-security.html

[xi] https://www.prnewswire.com/news-releases/edge-computing-market-worth-672-billion-usd-by-2022-654465673.html

[xii] https://www.ifrs.org/issued-standards/list-of-standards/conceptual-framework/

[xiii] https://sdgs.un.org/goals

[xiv] https://www.internationalinsurance.org/

[xv] https://www.internationalinsurance.org/insurance-development-forum

[xvi] https://www.unepfi.org/psi/

[xvii] https://www.weforum.org/

[xviii] https://guardtime.com/

[xix] https://www.precedenceresearch.com/blockchain-iot-market

3.2021

David Piesse
CEO, DP88

About the Author:

David Piesse is CEO of a family office, DP88, specialising in InsurTech initiatives in Asia - www,DP88.com.hk. David has held numerous positions in a 40 year career including Global Insurance Lead for SUN Microsystems, Asia Pacific Chairman for Unirisx, United Nations Risk Management Consultant, Canadian government roles and staring career in Lloyds of London and associated market. David is an Asia Pacific specialist having lived in Asia 30 years with educational background at the British Computer Society and the Chartered Insurance Institute.