MARSH

INSIGHTS | OCTOBER 2018

Internet of Things: Limitless Connections – and Ways to Fail

CMT Risk Considerations in the World of Hyper-Connected Networks

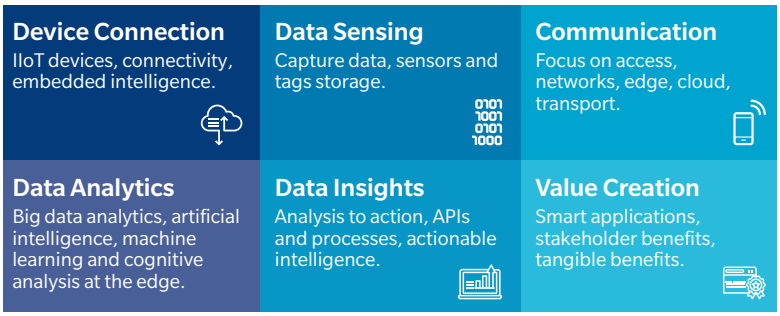
One of the most transformative technological advancements to develop in recent years is the Internet of Things (IoT). While it now touches nearly every industry, the IoT brings particular opportunities and challenges for those in the communications, media, and technology (CMT) industry.

IoT has been popularised with the emergence of "smart" devices, be they watches, lights, speakers, and even kettles. However, IoT has applications that are far beyond the consumer sphere, connecting the world in ways that were inconceivable not long ago.

IoT creates value by connecting devices and allowing users and companies to undertake the sensing, communicating, and analysing of the information they collect, store, and transmit (see fig 1).

FIGURE 1 IoT Value Creation

SOURCE: I-SCOOP OLIVER WYMAN ANALYSIS



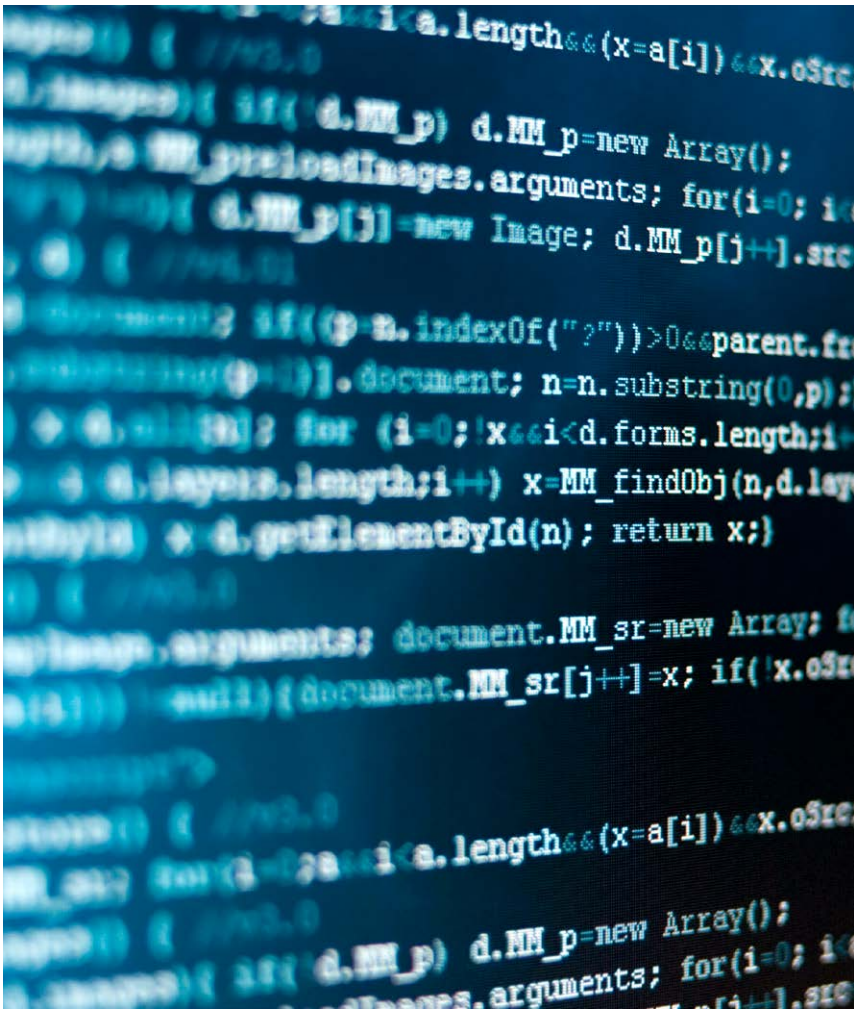
“IoT refers to the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity, enabling these objects to connect and exchange data.”

Brown, Eric (13 September 2016). "Who Needs the Internet of Things?"

Every new technological advance brings risks and rewards. New risks are created, some existing risks are amplified, and others modified. It is only organisations that manage and mitigate these risks that will be able to take advantage of the opportunities afforded by IoT.

Oliver Wyman analysed the number of connected devices that could be integrated into the IoT ecosystem and, despite variances between the number of devices that will be in use in the years to come, all measures point to extremely high growth rates. IoT is certain to be a high-growth area and investment opportunity for organisations in the next 5 to 10 years.

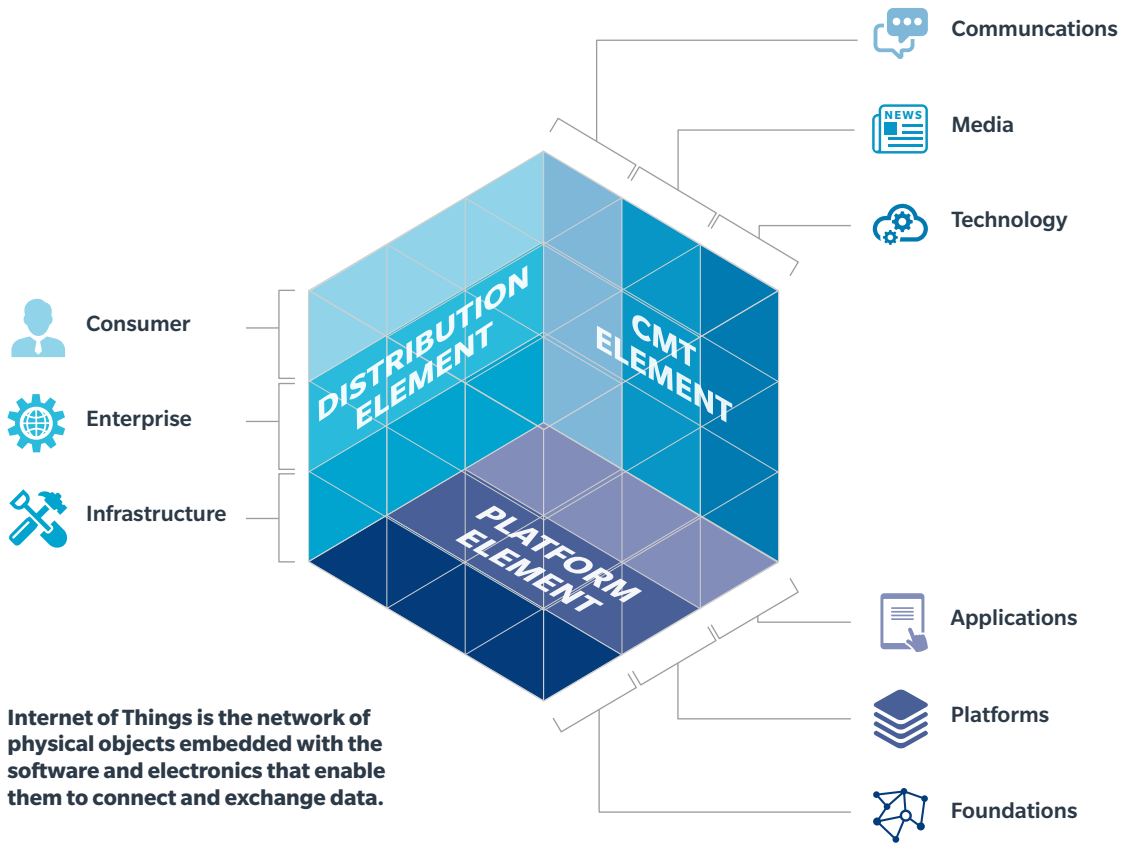
While rapid growth over the next 10 years is forecast, there are several predictions that mark the next two years as a tipping point in what could be exponential growth in the use IoT devices.



Risk Perception – Understanding the Risk

FIGURE 2 IoT Elements

SOURCE: MARSH ANALYSIS



The IoT Universe

While the potential for both new opportunity and new risk in IoT is evident, for many it is still a confusing space. When we peel back the layers, IoT is a simple concept: it is a collection of things connected by the internet. However, to enable and utilise these connections, there is a whole ecosystem involved in what could be called the 'IoT universe' – and many are unware of the part they play in this multi-layered universe, and how their position influences their perspective.

The IoT universe encompasses its use, operating systems, and the organisations using and developing the network(s). The elements of the IoT ecosystem interact to create a dynamic risk matrix. By understanding their position in the matrix – as part of the platform, CMT, and/or distribution sector – companies can be more aware of the risks they face.

A: Platform Element

Broadly speaking, the IoT platform element can be split into three main segments: applications, platforms, and foundations.

'Applications' refers to the ways IoT is used. The 'Platforms' segment is the software used to talk to the device. At the 'Foundations' of IoT we see the hardware manufacturers; the infrastructure providers, such as cloud computing services; connectivity services; and distribution partners.

B: CMT Element

Risks manifest themselves differently for each CMT sector. Risk stakeholders need to understand the impact that disruptive technologies, their applications, and related risk management priorities, have on their sectors, while balancing the need to invest in and develop enabling technologies. (Figure 6 further explores these considerations by CMT element).

C. Distribution Element

In addition to the platform element and CMT element specific risk considerations, the potential effects of a loss scenario are also differentiated by the distribution channel in which an organisation sits: namely consumer, enterprise, or infrastructure.

Organisations are likely to face effects from a blend of all three distribution channels, though depending on the scenario one channel will likely be a dominant consideration. (This is outlined in more detail in Figure 7).

FIGURE 3

A: Platform Element

SOURCE: MARSH ANALYSIS

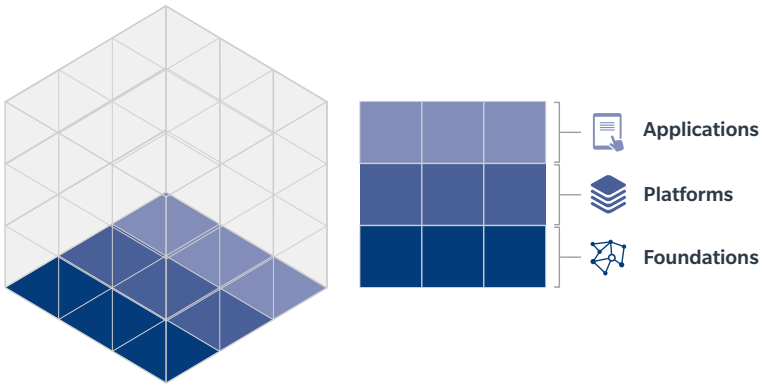


FIGURE 4

CMT Element

SOURCE: MARSH ANALYSIS

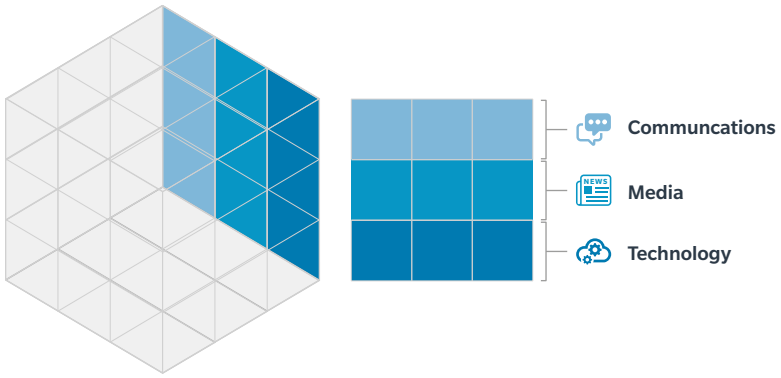


FIGURE 5

Distribution Element

SOURCE: MARSH ANALYSIS

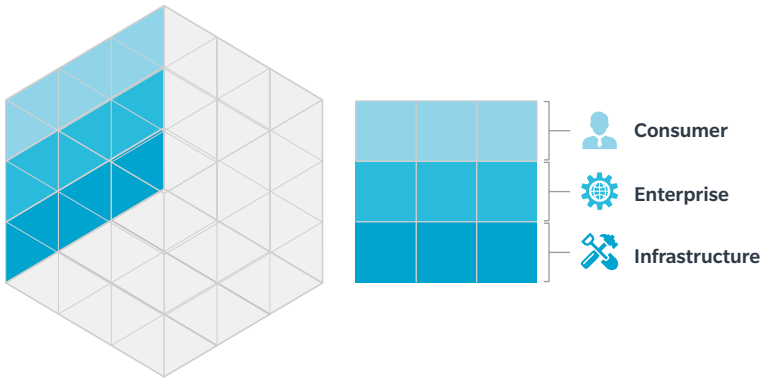


FIGURE 6

B: CMT Element Considerations

SOURCE: MARSH ANALYSIS

Communications

- Network infrastructure becomes even more important.
- Network continuity becomes vital to multiple sectors, which amplifies loss scenarios.
- Exposure to new sectors, new risks, and evolution of existing risks.
- Risk professionals need a deeper understanding of liability within the complex IoT network environment.
- Further push into advanced services.
- Increasing roll out of physical network infrastructure on a smaller-scale level (such as smaller WiFi devices).

Technology – Hardware

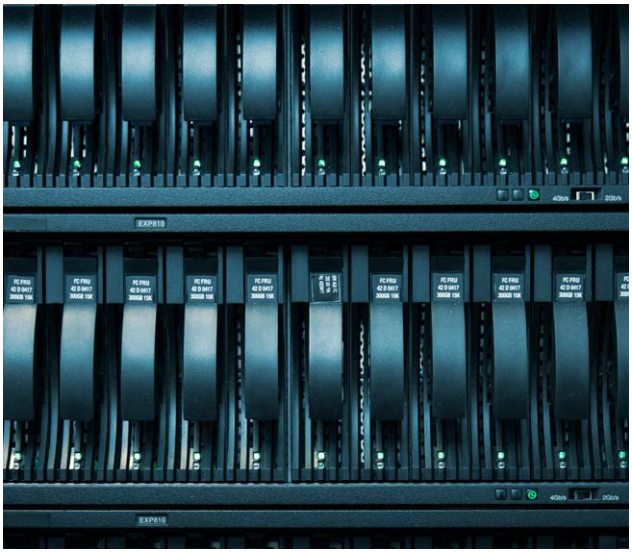
- Significant movement from hardware into services creating more "soft-tech" risks including software, denial of access/service, and transfer of malware.
- Potential for mega-scale global aggregated losses caused by a single vulnerability. This can evolve into non-damage business interruption, physical damage business interruption, terrorism, and general breach of contract scenarios.
- Increasing reliance on robust and evolving security standards in a rapidly evolving operating environment.

Media and Entertainment

- Organisations may face increased privacy issues relating to use of smart devices, AI and machine learning, and big data in better profiling consumers and targeted marketing.
- Increasing reliance on real-time and faster-moving content generation, ad campaigns, and other marketing techniques.

Technology – Software/IT Services/Internet

- Exposure to new risks and requirements in industry sectors, such as the auto sector and associated recall risk.
- Increased physical exposures where software/services can present physical damage and bodily injury losses.
- Complex joint venture and partnership arrangements with customers and service providers.



New risks are created, some existing risks amplified, and others modified.

FIGURE 7

C: Distribution Element Considerations

SOURCE: MARSH ANALYSIS

	Consumer	Enterprise	Infrastructure
Anticipated large-scale effects	• Increasing potential for bodily injury and third-party physical damage. • Invasion of privacy. • Evolving data and network security complexity.	• Significant amplification of errors and omissions (E&O) exposures due to increasing potential for frequency and severity of complex losses.	• Increasing contract size and reliance on IoT for numerous large infrastructure projects and operations.
Risk management	• Increasing exposure to consumer risks and related liability exposures. • Industry and consumer regulation.	• Impact on contractual risk management and transfer strategies.	• Potential for more onerous contractual demands and heightened risks (in both project and operational phase). • Complex joint ventures and project risks.
Insurance management	• Increasing product and public liability exposures. • Increasing product recall and E&O exposures. • Exposures to consumer regulations and related litigation (such as consumer protection, and privacy).	• Exposure modelling and setting of appropriate limits. • Incorporating contractual risk and terms and conditions accordingly. • Ensuring insurance portfolio is aligned and stress-tested.	• Requirement for ring-fenced and/or increased insurance limits. • Aggregation issues for (re)insurance markets. • Total global market capacity versus potential global aggregate exposures.
Tactical insurance challenges	• Border between general liability and tech E&O/ cyber is blurred. • Introducing new niche exposures into the mix (such as medical malpractice, diagnostics, construction, financial, pollution/environmental liability). • Level and extent of first-party coverage (such as costs, mitigation, notification).	• E&O limits may not be sufficient. • Infrastructure exclusions or limitations. • Service/supply chain management and risk transfer. • Level and extent of available CBI coverage (suppliers and customers).	• Terrorism exposure. • Property damage business interruption exposure. • Increased cyber and extortion exposure. • Contractual liability management and treatment.

Combined Risk Matrix Position

Understanding where in the IoT matrix an organisation sits is key to developing robust risk mitigation and transfer strategies.

The matrix can be used for any activity with a link to IoT to understand, categorise, and begin to mitigate the risks of operating in the space.

For example, a telecoms operator may have exposures which span across multiple dimensions of the matrix.

Consider a telecom operator that provides connectivity services for IoT devices that are used by businesses to monitor their sites across a region. The company would be located in the matrix by its three primary risk considerations:

- Platform: Foundation, due to the provision of IoT "building blocks".
- CMT: Communications, due to the nature of the business.
- Distribution: Enterprise, due to services being provided to businesses.

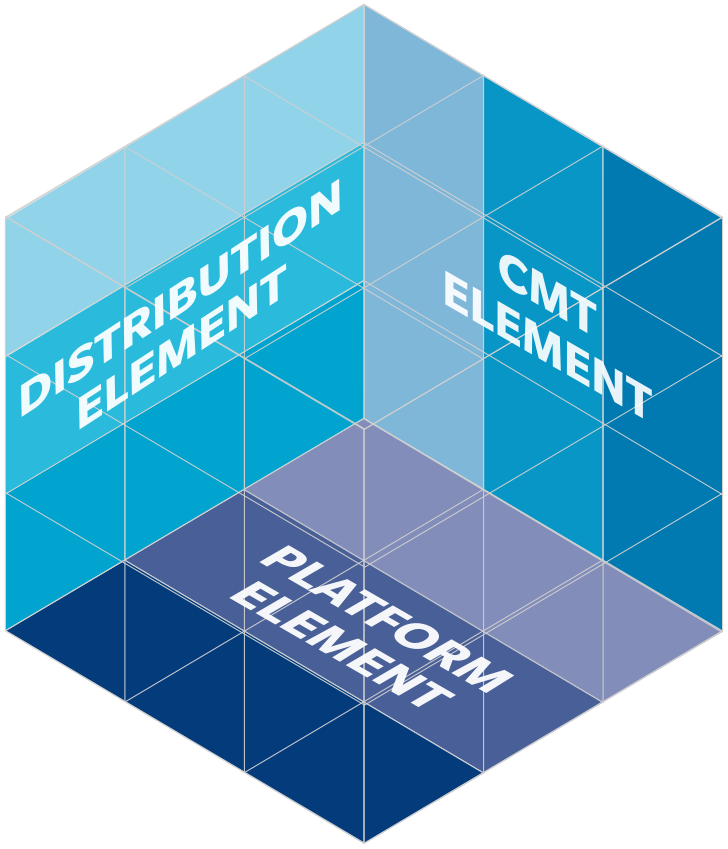
This shapes the risk management strategy for this exposure. However, the same company provides a software platform to industrial customers to understand their supply chain better. Now, the placement on the matrix changes:

- Platform: Application, due to the activity of supply chain monitoring.
- CMT: Communications, due to the nature of the business.
- Distribution: Infrastructure, due to services being provided to typically larger, more complex clients.

This shifts the position within the risk matrix; therefore the considerations for this activity will be different for the same company.

Or consider an app company that develops a product which users can install on their smartphones to monitor the whereabouts and vital statistics of their pet.

- Platform: Platform, because the company provides the software which interacts with a third-party device.
- CMT: Technology, due to the nature of the business of developing software.
- Distribution: Consumer, due to services being provided to individuals to monitor their pets' health.



Core Risks

At their core, IoT systems allow enterprises to make value-adding decisions in real time, with increased flexibility regarding their approach to efficiency, cost reduction, and risk modification.

It's important, however, to understand that IoT is a double-edged sword: It also increases the loss potential for existing risks as well as introducing new ones. In addition, technologies that are not fully secured present the potential for manipulation of data and automated controls.

In Marsh's *2018 Global Communications, Media, and Technology Risk Study*, 65% of survey respondents viewed the IoT as a growth opportunity over the next three to five years, with nearly half saying that their organisation is already engaged in the IoT universe by either creating or providing products and services.

There may be, however, a lack of understanding of the full range of risks presented by being part of an IoT device or system. Companies would benefit from doing even more to understand and evaluate their IoT involvement, with specific emphasis on new risks created.

Three Core Risks

There are three core risks groupings that any organisation will need to understand, manage, and mitigate:

- Contractual liability and risk ownership.
- Supply chain risk.
- Data, network security, and resilience.

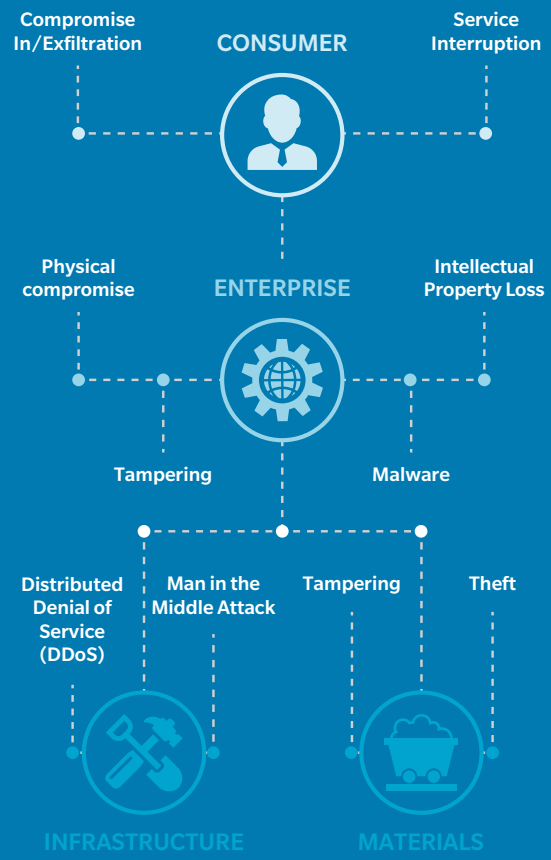
Contractual Liability And Risk Ownership

Understanding where liability attaches and detaches, as well as who owns the risk, is a priority no matter where in the IoT universe an organisation sits. The evolving risk landscape impacts both the need for risk transfer and its availability. In Marsh's *2017 Global Communications, Media, and Technology Risk Study*, 40% of risk professionals noted that contractual demands have a very high or the highest impact on the design of their insurance programmes, with more customers requesting increased limits of liability. Other reports have also highlighted that many companies have fallen behind on assigning accountability; with 38% of respondents to one admitting that no one is responsible for reviewing third-party risk management policies and programmes.

The IoT is highly vulnerable to network failure, security failures, and privacy breaches. However, only 19% of our 2018 respondents reported seeing demands of higher limits of liability being pushed into their contracts. Conversely, 50% of respondents cited bodily injury — the lowest risk of IoT – as an area where liability has been pushed. As well as contractual risk, the IoT may present complexities relating to public and product risk as well as more niche areas such as product recall, invasion of privacy, and regulatory risk. Determining how these liability risks attach and detach will be challenging.

FIGURE 8 Interplay of risks in IoT supply chain

SOURCE: SANS.ORG[1]



1. Sans. Combatting Cyber Risks in the Supply Chain, available at https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252 p4, accessed on 23 April 2018.

Supply Chain Risk

According to a SANS Institute Survey, it is estimated that up to 80% of data/network breaches may originate in the supply chain.[2] Disruptions to the supply chain are an increasing risk compounded by the highly international nature of technology supply chains and the lack of globally agreed norms for security standards. This risk is amplified by organisations not actively monitoring their IoT risk exposure. The *The Internet of Things (IoT): A New Era of Third-Party Risk* report found that only 28% currently include IoT-related risk as part of third-party due diligence, and 49% of organisations keep no inventory of IoT devices. [3]

Every new device added to an IoT-enabled ecosystem is a new vulnerability to the environment as there is an additional opportunity for malicious actors to access the network. As many of the devices being connected to networks are mass-produced, low cost — potentially low security — and unregulated (especially in the consumer segment), it may be easier than ever for a hacker to access major infrastructure through something as simple as WiFi-enabled light bulb.

Figure 8 outlines the interplay of risks in the IoT supply chain. At every stage of the supply chain there are ways in which malicious actors can access the network (see Figure 5). Once accessed, they can then infiltrate any other part of the ecosystem. "Once an IoT device is compromised," warns the FBI, "cyber criminals can facilitate attacks on other systems or networks, send spam emails, steal personal information, interfere with physical safety, and leverage compromised devices for participation in DDoS attacks."A challenge within the supply chain is the sheer quantity of data being processed, transmitted, and stored across the network. This means that it is difficult for organisations to know if there has been a breach within the network, especially if there is an aggregation of small breaches that don't trigger an alert. Coupled with the lack of risk ownership in the dispersed network, risk management becomes increasingly problematic as each party relies on others in the supply chain to manage the risk for them. This approach amplifies the vulnerability of IoT.

Data, Network Security, and Resilience

One of the main opportunities of IoT is the ability to collect and process vast amounts of data. When sensors are paired with the analytics of machine learning and artificial intelligence, valuable insights can be generated to inform decision makers on anything from the optimal traffic light sequencing for an urban area to targeted advertisements that drive behaviours in individuals. It is estimated that 2.5 billion gigabytes of data are generated every day, and that data production is exponentially increasing every year. As more data is produced, there are more opportunities for breaches to occur. For example, hackers could steal, tamper with, and corrupt data; software and programming errors may lead to information being leaked; or human error could result in breaches. In all of these scenarios, from malicious actors to errors and omissions, sensitive personal information could be affected, which further heightens the risk.

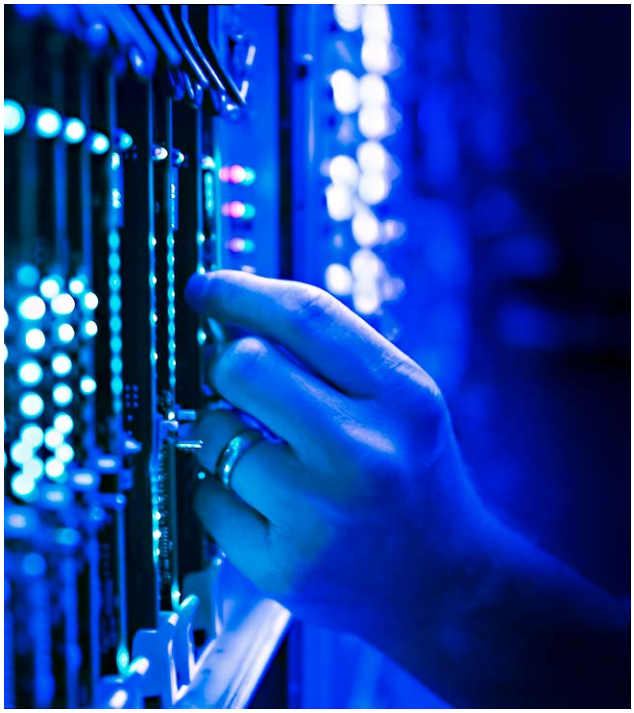
The need for organisations to ensure robust protection of their networks and the data contained within them has never been more important — but has also never been as challenging. Data illegally harvested by criminals could be used in a variety of ways, such as commuter-journey information to understand when an infrastructure attack could have the most impact; financial information being used to steal money; sensitive technical data from an industrial process for blackmail and extortion. The value of data is further increased by the analytics applied to it — and so as data is aggregated and processed, the value to potential bad actors increases.

The securitisation of data should sit high among boards' priorities. While data breach and cyber-attack already rank highly, many more exposures can affect the security and availability of data, including data loss, data damage, failure of network security, and non-damage business interruption.

IoT creates a data security challenge for organisations because it heightens the vulnerability for data breaches which, in turn, exposes them to more stringent regulatory enforcement action. Furthermore, many IoT devices, particularly those being used by consumers, are manufactured at a low cost and may not necessarily have adequate security features, which means that the most sensitive information may be the most vulnerable to attack. Indeed, the UK Government in March 2018 advocated "moving the burden away from consumers having to secure their devices and instead ensuring strong security is built into consumers' internet of things' (IoT) products by design".[4]

Many see data breach only as the result of malicious actors, however it is just as likely — if not more so — that a non-malicious event or an error or omission is the cause. These can range from software programming errors; loss of infrastructure, such as power or WiFi connection; untargeted malware, to a loss at a key service provider, such as a cloud computing provider. The outcomes of such partial or full interruptions to IoT services and networks could be significant and highly complex.

2. Sans. Combatting Cyber Risks in the Supply Chain, available at https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252, accessed on 23 April 2018.
3. Internet of Business. Serious IoT data breach likely by 2020, say risk professionals, available at https://internetofbusiness.com/iot-data-breach-third-party/, accessed on 23 April 2018.
4. UK Government. Secure by Design, available at https://www.gov.uk/government/publications/secure-by-design, accessed on 23 April 2018



IOT PROVIDER CONCERNS

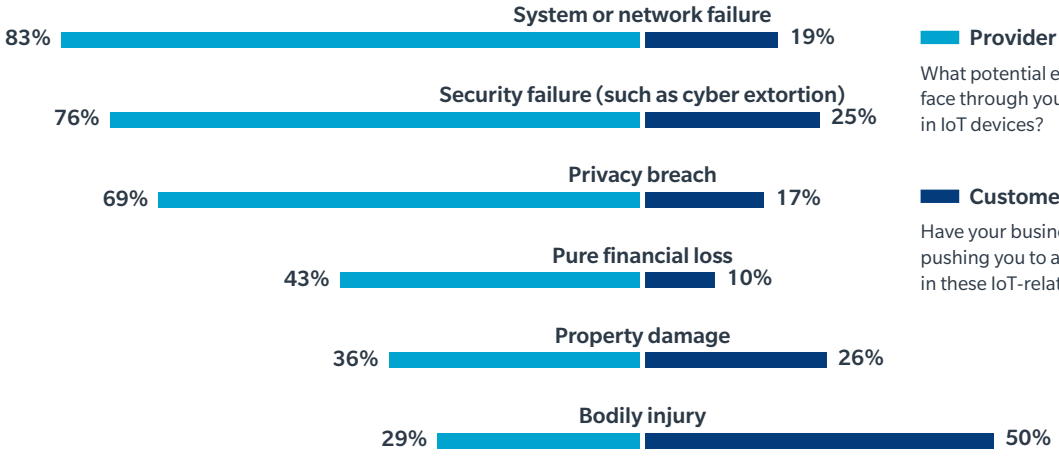
The top three IoT loss exposures cited by respondents are related to cyber events: system or network failure, security failure, and privacy breach (see Figure 9). Well under half of the surveyed organisations cited pure financial loss (43%), property damage (36%), or bodily injury (29%) as exposures.

Using bodily injury as an example, the failure of a connected device — through a production error, a cyber-attack, or other cause — has the potential to cause injury. The reality of this can be inferred from the fact that half of respondents said their partners are asking for increased protection against the risk. Yet many IoT providers seem not to be making the same connection that their customers, suppliers, and other partners are.

FIGURE 9

System operation and security dominate IoT provider concerns; users increasingly concerned with physical risks.

SOURCE: 2018 COMMUNICATIONS, MEDIA, AND TECHNOLOGY RISK STUDY



Theoretical Loss Scenarios

The connected risk landscape of IoT creates, amplifies, and modifies risks. Far from theoretical, attacks on IoT devices are common, with the Mirai and Repear attacks recent examples. Indeed, cybersecurity firm Symantec found that the average IoT device is attacked once every two minutes at peak times.

As an emerging risk consideration for organisations, below are some possible loss scenarios that CMT companies may face through exposure to the IoT.

Scenario	
Type	Risk creation
Overview	A technology component manufacturer designs and manufactures low-energy consumption IoT devices that are traditionally used in location services, but are then used to form part of an autonomous vehicle. The devices themselves form a broader part of the overall safety and navigation systems.
What goes wrong	After a period of time it is deemed that the devices can fail to perform under certain conditions, leading to a large recall for the auto manufacturer. Remote firmware updates are not able to deal with the issues.
Outcomes	Event involving multiple devices, networks, and companies. Public relations incident. Consequential financial losses for loss mitigation, subsequent recall, and investigation costs and loss of earnings.
Considerations	While not an end-manufacturer, the company may have needed to comply with specific contractual (indemnity) conditions and such as purchasing product recall insurance. Previously the company had a pure financial loss (or E&O) exposure to its B2B customer (the end-manufacturer). Within this scenario the manufacturer may seek to take control of the recall incident and then subsequently demand damages for costs incurred. Such recall events can significantly exceed the value of the contract/services/devices provided.

Scenario	
Type	Risk amplification
Overview	A marketing/media services company uses its proprietary app to extrapolate significant volumes of data through an IoT network consisting of consumers' mobile devices.
What goes wrong	The company is accused of mass invasion of privacy, as its app has been recording volumes of data not known by the consumers (such as conversations and location data).
Outcomes	International class actions result in significant legal costs, regulatory investigations, and the potential for fines and penalties.
Considerations	• Legal defence costs and damages. • Regulatory costs and exposures. • Reputation and brand damage.

Scenario	
Type	Risk modification
Overview	A software company is strategically engaged by an equipment manufacturer to provide software, as well as ongoing cloud-based IT services, to support IoT devices. The devices are used in numerous applications and sectors including automotive, industrial, and telecommunications.
What goes wrong	A transfer of malware event ensues where malicious code (which was inherent in the firmware) becomes active and spreads across multiple networks, resulting in network shut-downs, security incidents, and interruption to services.
Outcomes	International security incident involving multiple parties, networks, systems, and services. The event leads to potential subsequent fraud and extortion (criminal actors attempting to take advantage of the confusion and vulnerabilities), as well as significant costs incurred by the multiple affected companies.
Considerations	• Highly complex loss mitigation procedures. • Crisis management and public relations. • Potential for a loss event to manifest into further events and losses (incurring consequential losses for B2B customers).

Scenario	
Type	Super-convergence — black swan event
Overview	A significant IoT event results in a complete loss of infrastructure within a large urban area.
What goes wrong	There is a power supply infrastructure failure caused by a non-malicious fault within the IoT monitoring network, leading to blackouts across a large and dense urban area.
Outcomes	Massive power outage resulting in partial to full secondary infrastructure failure (such as telecommunications, water, gas, transport, and sewage), as well as consequential impact on private business and society in general.
Considerations	Such a black swan event could incur financial losses outside the realm and scale of the global insurance and reinsurance industry.

Opportunities

In the Marsh's *2018 Communications, Media, and Technology Risk Study*, 65% of respondents cited IoT devices as an opportunity for their organisation over the next three to five years. In addition, IoT offers organisations a number of opportunities for risk mitigation and increased efficiency. Risk managers are in prime position to lead conversations on how technology can be leveraged to provide solutions to emerging risks.

IoT offers organisations a number of opportunities for risk mitigation and increased efficiency.

Real-Time Asset Tagging

Radio-frequency identification and low-power wide area networks (LPWAN) can be used for asset tracking where small amounts of data are transmitted over a wide area. By using LPWAN, people and assets can be pinpointed at locations within a given area, such as a manufacturing plant. This information can then be combined with other data collected to help optimise decision making and tracking throughout an industrial process. Businesses may also use this technology to track the location of employees and visitors in an office, which can help to account for people in the event of an emergency evacuation. Another use of this technology could be to track livestock location and health status, allowing farmers to spot issues before they become serious.

The collection of data for renewals insurance could potentially be faster and more efficient, and could be done in real time as opposed to annually. Companies that work in Economy 4.0 or the gig economy could leverage this real-time tracking technology to know the location and behaviours of their operators, and generating an instant reading of the risk profile of those using the platform.

Health and Safety

The monitoring of workers and workspaces is not a new concept in health and safety. Indeed, remote monitoring has been possible for a number of years. However, real opportunity is created by IoT when devices are able to interact with one another without the need for human involvement.
This is particularly useful when used in conjunction with hazardous processes.

IoT could also help extend the life of machinery. Equipment can be automatically adjusted based on the information received from sensors, allowing for its lifespan to increase and preventing the need for maintenance workers to enter into potentially dangerous spaces to rectify faults.

Similarly, wearable devices on workers can help determine their exposure to noise, chemicals, and vibration levels in construction and manufacturing industries or, conversely, could be used to monitor how sedentary a worker is in an office situation.Such information can be aggregated to discover trends, and then inform risk management strategies. Additionally, it can help to monitor in real time the status of a workforce and to allocate workers effectively so that fewer accidents occur in the workplace.

Supply Chain Management

IoT has the power to revolutionise supply chain management, and is an area that many logistics and retail companies are investing in.

IoT offers businesses the opportunity to track assets and improve vendor relations, inventory management, and maintenance schedules. Using data collected through asset tracking, companies will be able to adjust production schedules and have greater insight into quality control, stock management, and delivery management.

For inventory management, IoT sensors are able to provide real time, highly accurate inventories that in many cases are free from human error. IoT can be used to track and triage orders, and even reorder stock that is running low. Smart sensors can be used on manufacturing floors to manage planned and predictive maintenance and prevent down time that can prove costly.

Auto Risk Management

It is estimated that there are 60 to 100 sensors in an average vehicle, with analysts predicting that there will be up to 200 per vehicle by 2020.[5] In 2016, the average modern vehicle contained 150 million software lines of code.[6] These sensors and software allow for increased insights into exposures, and improve risk management. For example, IoT allows for real-time monitoring of the state of repair of fleet vehicles and can automatically flag vehicles for repair before the fault becomes more serious. A connected fleet allows organisations to get better products to their customers; move people and goods more effectively; and optimise vehicle performance.

Economy 4.0 Platform Risk Management

The ability to formulate a clear picture of risk is a challenge for Economy 4.0 organisations, which operate platforms of exchange where services are offered by contingent talent. For example, a company using independent couriers to deliver a product, and offering them the ability to buy their own insurance for the work they undertake on the platform, is not able to see which couriers drive more safely than others via a claims history. IoT technologies can be leveraged to provide the platforms with information regarding driver safety. This information can be then used to differentiate service providers on the platform. For example, better performers can command a higher price on the platform for their services, or they may be charged a lower premium for insurance cover.

5. Automotive Sensors and Electronics Expo 2017, available at http://www.automotivesensors2017.com/, accessed on 23 April 2018.
6. McKinsey. Rethinking Car Software and Electronics Architecture, available on https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/rethinking-car-software-and-electronics-architecture, accessed on 23 April 2018.

CONCLUSION

The hyper-connectivity of networks and devices through IoT brings with it a need for organisations to better understand and manage risk. CMT companies that previously had exposures in only one industry are now likely exposed in new sectors where they have little or no experience. These connections across distribution channels, industries, and elsewhere mean that traditional strategies for managing insurance need to be re-evaluated.

CMT companies have undergone rapid transformations in their overall risk landscapes from the tangible to intangible — and with the IoT, their intangible risks can manifest physically as well as non-physically, creating a further layer of complexity. For risk mitigation, a complete understanding of the corporate insurance portfolio and the specific cover it provides for disruptive technology is essential.

The survival and prosperity of organisations will depend on their ability to understand the risks they are exposed to and are creating. CMT companies in particular, will need to understand where in supply chains their products are being used and the industry-specific considerations they must address.

One way to help better understand your IoT risks is to consider where on the IoT matrix your organisation — or a specific function — fits. Use this positioning as you consider the risk implications and strategies presented by various scenarios.

For companies whose products have broad applications in numerous industries, this will be an intricate and challenging exercise. However, the opportunity to use risk management as a business enabler and innovation driver is one that should be welcomed.

For further information, please contact your local Marsh office or visit our website at marsh.com.

CARRICK LAMBERT
+44 (0)20 735 75480
carrick.lambert@marsh.com

SAM TILTMAN
+44 (0)20 7357 3255
sam.tiltman@marsh.com

BENJAMIN HINDSON
+44 (0)20 7178 4479
benjamin.hindson@marsh.com