The "Internet of Things" at Risk

By Gilles Hilary , INSEAD Professor of Accounting and Control, and Rudi Spaan , President and CEO AIG Hong Kong

Internet-enabled devices improve productivity and help us achieve greater innovation, but there are three major risks that could unravel it all.

It is **estimated** that 90 per cent of the world's data has been generated over the past 2 years. Every second, the data equivalent of 150 million books is created. A large part of this expansion is attributable to the Internet of Things (IoT), the network of "smart" physical devices that collect and exchange data.

When most people think of internet-enabled devices, examples such as Fitbit and Apple watches naturally come to mind. But these products are quickly being outnumbered by others that are less familiar. These new devices capture data from industrial plants, machines and even the human body, then transmit it elsewhere over the internet or another network where it can be stored and analysed to enable better decision making.

There are countless applications for virtually every industry related to construction and real estate, from telecom to energy. Many of these applications are designed not just for convenience, but also for safety. For

example, electrical systems can be equipped with sensors that detect wiring failures, warning technicians of fire hazards before the fire can occur.

But while the IoT may herald a period of unprecedented opportunities, it is also one of unprecedented complexity. These devices pose new **challenges** for managers and risk specialists who need to be connected with their R&D departments as never before. We see three big new IoT dilemmas that society needs to resolve.

Data Confidentiality

The first is confidentiality. Consider the use of smart TVs. Unlike the old-fashioned projectors, they are connected to the internet. They are operating behind the firewall and are plugged into sensitive networks, often without necessary care. What happens when sensitive information is leaked? More fundamentally, all IoT pioneers must grapple with well-known concerns over privacy — how to balance expectations of privacy with the inherent need to collect and analyse data in ways that harness the true power of the IoT.

Personal data is easily shared by various companies and devices creating all sorts of potential privacy concerns. For example, workout data from one device can be connected to insurance company systems to calculate health and life insurance premiums.

Most insurance companies have already started offering better rates to those who can demonstrate more healthy lifestyles. The IoT means behaviors can actually be tracked and validated with much greater precision. But what about individuals who cannot afford or simply refuse to wear IoT devices based on privacy concerns? This raises key questions for insurance companies, elected officials and regulators.

Data Connectivity

There have been numerous high-profile cyber-breaches which have caused damage. But the risk takes on a different dimension when so many devices are connected. In fact every node on the internet is a potential access point for someone unscrupulous or malevolent. As a society we are installing billions of connected devices in everything from aeroplanes to flood defence systems.

A connected and automated system can improve the efficiency of a town's electricity grid. But it also gives a hacker a way to shut down that electricity

grid from their own computer.

Even without any malfeasance, this connectivity also creates issues in case of catastrophic outages. If an earthquake massively degrades network capacity in a large area, the use of smart lifts for building evacuation might be impacted. Urgent payments for medical care or intelligent traffic lights could also be crippled.

Data Liability

The biggest risks for the insurance industry during the IoT revolution, however, center on increasingly complex questions about liability and cybersecurity. If a sensor fails to detect a potential problem in a machine, it might be difficult to determine who is at fault? If a semi-autonomous truck is involved in an accident, resolving who is responsible takes on multiple dimensions. This could also depend on the jurisdiction in which the vehicle is driven. With so much data collected and shared across a host of machines, someone needs to be accountable for accuracy and security. Now that everything can be monitored, failing to monitor is an even greater risk.

There is also the ethical conundrum of how connected machines should be programmed to make decisions. We are not used to objects acting on their own and they might act in unexpected ways.

But more than that, so much of the potential of the IoT lies in the seamless transfer of data between devices. This will make it very difficult to associate an individual piece of data with an individual device, and to allocate responsibility for any failure.

The insurance industry has developed over centuries as a means of transferring risk of loss from one entity to another in return for payment. The effective transfer of risk is a fundamental pillar of the modern economy that relies on understanding contingencies. This process is going to become much more complicated in the near future.

Gilles Hilary is an INSEAD Professor of Accounting and Control and The Mubadala Chaired Professor in Corporate Governance and Strategy. He is also a contributing faculty member to the INSEAD Corporate Governance Initiative.

Follow INSEAD Knowledge on **Twitter** and **Facebook**

Find article at

About the author(s)

Gilles Hilary Gilles Hilary was a Professor of Accounting and Control at INSEAD and is now a professor at Georgetown.

Rudi Spaan Rudi H. Spaan is the President & CEO, AIG Hong Kong; Head of Country Operations Hong Kong & Taiwan and Head of Client & Broker Engagement for the Asia Pacific region.

About the series

Corporate Governance

Established in 2010, the **INSEAD Corporate Governance Centre** (ICGC) has been actively engaged in making a distinctive contribution to the knowledge and practice of corporate governance. Its vision is to be the driving force in a vibrant intellectual community that contributes to academic and real-world impact in corporate governance globally.

The ICGC harnesses faculty expertise across multiple disciplines to teach and research on the challenges of boards of directors in an international context. The centre also fosters global dialogue on governance issues, with the ultimate goal of developing high-performing boards. Through its educational portfolio and advocacy, the ICGC seeks to build greater trust among the public and stakeholder communities, so that the businesses of today become a strong force for good for the economy, society and the environment.

4