& Digital
Fellow @QUT PwC Chair in Digital Economy_Views are my own
Oct 19, 2017 · 7 min read

Risk Management Revolution

I had a dream. Risk management stopped preventing losses and started creating value. Could this become true?

We live in thrilling times. Opportunities and chances are literally thrown at us. A mainstream excitement spreads across our offices, shops and boardrooms. Disruptive innovations shake our workplaces, raise concerns at first, but are then quickly accepted. Embraced. Leveraged. Loved. Dragged by the enthusiastic passion of our entrepreneurial Millennials, we all want to be part of the Digital Economy. We connect, communicate, share, collaborate, regardless of our age. A general feeling of optimism seems to animate most of our organisations. In this thrilling environment, there seems to be less and less space for Risk Management (RM), the discipline of looking at the dark side of things. Is this true? Why?

The historical trajectory of RM is a very interesting story in itself (Quarantelli, 2000). It all started at the dawn of times, when people thought disasters (and associated risks) were essentially *Acts of God:* not much to do to prepare, just praying that the consequences would not be too harsh. The *Enlightenment,* with its rational perspective, brought a different approach: calamitous events were considered *Acts*

of Nature, against which some form of preparation was considered possible. The third industrial revolution increased our reliance on socio-technical systems and automation. Sadly, it also brought some of the worse industrial disasters in history (Seveso, Three Mile Island, Bhopal and Chernobyl) and led to the development of a new concept (see the *Normal Accident* and the *Disaster Incubation* theories, Perrow, 2000 and Turner & Pidgeon, 1997): crises and disasters were now conceived as *Acts of Society*, against which humans could, and had to, prepare. This turning point facilitated the development of RM as a new organisational function and research discipline.

As the short explanation above demonstrates, the changes that created fertile ground for RM to develop took years, centuries to materialize. Can we reasonably expect that the current, fast-paced environment could have a dramatic impact on the validity and appropriateness of traditional RM practices? What consequences can have on RM the wide-spread use of digital technologies in more and more components of our organisations; emergent, successful business models thriving in the Digital Age; and globalization trends that seem to never stop? As any organisational function impacted by the dynamics of the Digital Age, some of the basic assumptions of traditional RM seem to clash with the success factors of digital companies and platforms.

Four major hurdles

To understand how such a clash unfolds, let's look at four key features of both the Digital Economy and traditional RM and compare them (see table below).

Digital Economy	Traditional Risk Management
Focus on creating value for end-customers	Focus on preventing losses for organisations
Partner with your customers (value co-creation)	Separate from your customers
Flexibility and decentralisation	Rigidity and centralisation
Utilise and leverage idle assets	Idle assets only used if and when needed

1. ***The value dilemma.*** Let's mention one simple example: the Australian Cyber Security Centre 2016 Survey (ACSC, 2016, p. 17) ranks the top motivations for companies to invest in cybersecurity. The first five deal with *'protecting'*, *'preventing'* and *'complying'*. Only the last entry has some sorts of proactive connotation (*'gaining access to markets'*). This epitomizes risk managers' *bread and butter:* avoiding losses, or mitigating their impact. How long can this position be held in the age of *customer-value-at-all-costs*?

2. ***Customers, what customers?*** *Co-creating unique value with customers* is not only the title of an eminent book (Prahalad & Ramaswami, 2004) that illustrates the changing nature of competitive advantage, but also one of the leitmotifs when it comes to ruling the Digital Economy. Design thinking methodologies assume that no one better than a customer knows what a customer's needs are, and embed users in the creative process itself, by multiplying customers' touch-points as much as possible. In RM, customer touch-points are virtually non-existent, and the concept of separation (physical or virtual) permeates the ways in which companies manage risks. Can you currently imagine an airport designing their security screening procedures in collaboration with the passengers?

3. ***Centralised or decentralised?*** In an era where flexibility and decentralization play an essential role in allowing organisations to focus on their core business, while keeping costs low and customizing their products as much as possible, traditional RM still looks like a highly centralized organisational function. Traditional RM is in an apparent paradox with the Digital Economy: digital platforms (Alibaba, Amazon, etc.) share information with their partners (*symmetric information)* to provide highly personalized services to their customers (*asymmetric services*). In so doing, they leverage *network effects:* they look at expanding their networks first, and providing customized services after (for example Linkedin). Traditional RM, on the contrary, holds onto information (*asymmetric information,* think of the perceptions of *commercial-in-confidence* information) to create standardized mitigation strategies (*symmetric services*), which keep costs low (one-size-fits-all). RM looks at providing services first (risk mitigation strategies), with not much consideration for the networks of customers of reference.

4. ***Idle assets.*** Many successful platforms have made their fortunes by combining network effects with the potential of idle assets. Imagine the returns that companies such as Uber or AirBnB have secured by facilitating the utilization of idle cars and drivers or unused rooms and accommodation. In the traditional crisis management life-cycle (*prevention, preparation, response, recovery*) idle assets abound: besides prevention, equipment and resources are kept on hold until something goes wrong. Would a company constantly review their CCTV recordings if no security breach were detected?

Risk Management of the Future

So RM seems to have a problem with *value creation*, *customers*, *centralization* and *asset utilization*. Then what's next? Let's use a traditional *why, what, how* and *when* framework to suggest some possible responses (and attract criticism…).

> *Why?*

The why of RM of the Future will expand. As long as individuals, corporations or platforms will get involved in potentially risky operations (from a financial, performance, safety, or security perspective), there will be an appetite for risk mitigation. Will we be able to pursue the Utopian *zero harm?* Hard to say, and harder to achieve. On the one hand, digital technologies (AI for example) have a great potential for some exciting applications, intended to overcome the limitations of sub-optimal, man-made decisions. On the other hand, modern, emergent threats are more complex and interlinked (think of cyberwarfare or lone-wolf terrorism, just to mention two). And the magnitude of present-day natural hazards is growing, too.

The *why* of RM of the Future will expand to also include value creation for end-customers. In what form? Business intelligence, leverage of idle assets and trust management are three examples (see *how?* below).

> *What?*

A change in RM paradigm is necessary. In an attempt to provide a justification for physical security expenses and make corporate security more 'meaningful' for the board of directors, the concept of security return on investment (security ROI) has been introduced. However, its quantification (for instance, by calculating the *annualised loss expectancy—ALE,* see here for an example) is challenging, as it may require extensive amounts of data in order to yield reliable results. Moreover, physical security ROI can be largely based on likelihood estimates, which can be subjective or fluctuate over time. In the field of cybersecurity, security ROI is seen as even more complex. On this topic, nine years ago, Bruce Schneier wrote an interesting essay, which has been recently re-discussed, with similar conclusions: ROI does not seem the right metric to provide justification for cybersecurity spending.

Rather than thinking of loss prevention, modern RM should focus on adding value for end-customers, possibly co-creating value with them.

> *How?*

Among the four, this is the trickiest question. Based on the types of risks and domains, different solutions could increase the end-customer value yielded by organisational RM practices, tools and procedures. An example is **business intelligence**: by maintaining solid RM practices, organisations can better learn how they run and what impacts external agents have on them. This can ultimately lead to more efficiency. Again, cybersecurity constitutes an example domain, with data mining applications used to map security vulnerabilities as well as provide rich information about organisational processes.

Generally speaking, data produced through RM tools and practices can be considered **idle assets** that companies can leverage. RM has the potential to establish itself as an organisational function that produces strategic business intelligence. In modern organisations, risk managers should further develop data mining and business analysis skills. Can risk managers in retail shops be trained to analyse CCTV recordings to learn more about customers? Could airport safety inspections be utilised to capture data about weather, traffic on the tarmac or baggage handling throughput?

Finally, **trust management** is an area in which RM can produce strategic value. With appropriate corporate communication, companies can shape their risk managers' role around interacting with end-customers to strengthen reputation from solid RM practices as in, for instance, identity management. Similar to the transition from *Chief Information Officers* to *Chief Digital Officers*, a near-future shift from *Chief Information Security Officers* to *Chief Identity Management Officers* is an option.

The *how* of RM of the Future should also include **value co-creation:** for end-customers, together with end-customers. An example of this is from disaster relief. Research shows that *digital volunteering* has an increasing role in disaster management (McLennan, Whittaker & Handmer, 2016): volunteers, as victims of, as well as first-respondents to, disasters, offer their data (for example, from social media) to create meaningful information that assists institutions in disaster response. Together with value co-creation, adopting **collaborative approaches** (and overcoming hyper-competitive behaviours) will be essential for companies engaging in RM activities. Can we design digital/physical platforms in which members share information about common threats and 'receive' in exchange the most appropriate protection and response strategies? In this area, cybersecurity already provides numerous examples (for instance AusCERT).

> *When?*

Needless to say, now. The dynamics of the Digital Economy are fast, emergent, disruptive. To increase its relevance, RM has to act as quickly as possible.

The numerous examples here mentioned demonstrate that the shift towards the **Risk Management Revolution** has already started. Cybersecurity as a domain is in a good position to pave the way for other RM areas to follow.

. . .

At the PwC Chair in Digital Economy at QUT, we are currently conducting research to understand how strategic cybersecurity can become in the competitive landscape of the future. The expectation is that our findings will provide practical solutions to answer the *why, what, how* and *when* of the Risk Management Revolution.