

GAME ON – 5 TRENDS IMPACTING THE RISK LANDSCAPE

SUE TREZISE – *Sue-lutions Ltd*

Deloitte's recently published "The future of risk – new game, new rules" report profiles 10 trends that have the potential to significantly alter the risk landscape for companies around the world. The reports highlights new opportunities and new challenges leaders should prepare for and provides insights for risk practitioners to advise and support key decision makers.

This article summarises five of the profiled trends, selected because they most piqued the interest of this author, and also seemed most relevant to the New Zealand context. Not listed in any priority order, they provide a broad spectrum of emerging risk insight, helping to generate diversity and expansion in risk management thinking. Harnessing these trends will enable/support organisations to improve capability and resilience.

Trend #1 Cognitive technologies augment human decision-making

Driven by developments in artificial intelligence (AI) and easy access to huge amounts of data, smart systems will assist, and at times even replace, human-led risk management.

Applications of cognitive technologies include: technology embedded in a product or service to provide end-customer benefits; process applications to automate or improve workflow/operations and insight applications used to inform operational and strategic decisions across an organisation.

A specific example is managing social media risk using tools which scan social networks to discover and track an organisation's footprint; detect fraudulent social media accounts, unauthorised changes, and anomalous behavior on social account profiles; reduce potential liability from inadvertent posting of sensitive data; and demonstrate compliance with standards and industry regulations.

Forces driving this trend:

- Massive growth in the volume of data available to organisations
- Emergence of new and advanced AI-based algorithms
- Expanding pool of data science talent
- Adoption of behavioural analytics in risk management

Opportunities arising:

- Use of visualisation to analyse and communicate information in a human-friendly way to enable rational decision-making
- Upskill employees to enable more effective use of cognitive technologies to extract insights from data

Potential threats and pitfalls:

- Difficulty in implementing complex cognitive tools
- Lack of trust and assurance mechanisms for AI
- Human backlash against automated decision-making
- Unintended consequences of mistaken predictions

Trend #2 Controls become pervasive

In a sensor-enabled, hyper-connected environment, organisations will deploy pervasive controls as part of their products, services, and business models to monitor and manage risk in real time. Smart devices (also known as the Internet of Things (IoT)) equipped with a variety of sensors, communications, and computing capabilities serve as risk monitoring and enforcement points.

Continued on next page...

Examples include:

- ✓ Deployment of sensors into a truck fleet to track maintenance needs, driver safety, fuel usage, and other metrics in real time
- ✓ Wearable tags that can detect whether users have changed location or posture, have fallen down, or are experiencing high heat. Such tags enable real time monitoring of employees' working conditions with the aim of reducing workplace injuries.

Forces driving this trend:

- Declining cost, decreasing size, and increasing connectivity of sensors
- Advancements in sensor technology and analytics
- Growing adoption of workplace wearables

Opportunities arising:

- Automate compliance monitoring and reporting by embedding risk controls into business technologies
- Reduce cyber security and fraud risk by using sensor-enabled devices to implement identity access capabilities
- Improve traceability across the supply chain
- Manage risks introduced by customers by analysing their behaviour through real-time data feeds

Potential threats and pitfalls:

- Heightened exposure to cyber risks as business processes rely more heavily on the IoT
- Greater availability of data revealing risks in areas that were formerly considered safe, resulting in new obligations to manage those risks or increased liability
- Rising privacy concerns from employees, customers, and business partners
- Difficulty filtering relevant information from the noise, given vast amount of data generated

Trend #3 Behavioural science informs risk insights

Advances in behavioural sciences (study of human behaviour) will fuel efforts to understand risk perceptions, influence risk behaviours, and improve risk-related decision-making.

A specific example is the use of psychological profiling tools to ramp up computer security in the workplace. Such tools aim to identify workers who are most vulnerable to cyberattacks, based on their behaviour while checking and sending emails, and browsing the web.

Forces driving this trend:

- Increasing interdisciplinary research across fields such as cognitive science, psychology, economics, and neuroscience
- Growing popularity of behavioural economics to inform decision-making

Opportunities arising:

- "Design interventions" to help executives overcome the influence of cognitive biases in decision-making
- Improved systems for monitoring high-risk individuals in sensitive roles
- More effective risk, forensics, and financial transaction-related business processes

Potential threats and pitfalls:

- Risk of regulatory action in case of perceived misuse of behavioural interventions
- Backlash from employees and executives who see behavioural interventions as an impingement of free will

Continued on next page...

Trend #4 Risk transfer broadens in scope and application

Risk transfer instruments, such as insurance, contracts, and novel financial instruments, will increasingly be used by organisations to protect them from a wider range of risks – cyberattacks, climate change, geopolitical risks, terrorism, business disruptions, and more.

Forces driving this trend:

- Growing instances of “mega-impact” events such as cyberattacks, political unrest, and climate change, and their growing financial and reputational impact
- Increasing globalisation and the rise of a networked economy leading to cascading risks
- Inability of organisations to completely eliminate risks through preventive controls

Opportunities arising:

- Evaluate risk transfer instruments as an option to achieve business continuity and more predictable performance
- Develop clear and stringent risk-sharing clauses in all partner contracts, and consider collective insurance with partners to address shared risks

Potential threats and pitfalls:

- Potential for conflict, litigation, and disputes with customers, partners, and suppliers over risk-sharing agreements
- Inability to determine the appropriate insurance premium for various risks
- Becoming “over-insured” or purchasing insurance in noncritical areas

Trend #5 Reputation risks accelerate and amplify

To survive in a hyper-connected world dominated by mobile devices, social media, and evolving expectations from society, leaders will proactively address accelerated, amplified risks to their organisation's reputation.

Examples include:

- ✓ A media conglomerate which fired its head of communications for an offensive personal social media post (which went viral in a matter of hours) in an effort to prevent further damage to its reputation
- ✓ Food safety incidents which cause significant reputation loss and revenue impact for food and beverage companies. The impact on a company's reputation is often intensified due to the negative attention received through social media channels

Forces driving this trend:

- Social media creating a more connected, networked world where information is rapidly amplified
- Mobile technologies creating hyper-availability in which people are always available and connected
- An upsurge of socially conscious consumers, and growing consumer activism, putting pressure on businesses to be socially responsible and transparent
- Multichannel marketing strategies built on social platforms allow for greater interactivity for consumers and less control for brands

Continued on next page...

Opportunities arising:

- Develop new capabilities for proactive brand-related crisis management
- Initiate targeted campaigns and develop an external ambassador program to nurture external brand advocates
- Foster a more risk-intelligent culture to help employees see the reputation implications of their actions

Potential threats and pitfalls:

- Personal online activity of employees can cause reputational damage to the organisation
- Organisations may be forced to respond to risk events in haste without fully investigating the situation

For more details, and to review Deloitte's other five trends, check out:

<https://www2.deloitte.com/us/en/pages/risk/articles/future-of-risk-ten-trends.html>



SUE TREZISE – Sue-lutions Ltd

Sue Trezise has over 12 years experience providing risk expertise and advice for government and organisations on strategic, enterprise and operational risk management. An experienced facilitator, Sue assists communication between technical experts and non-technical stakeholders and makes managing risk practical and effective.