Aon | Professional Services

Lessons learned for professional service firms: technology & cyber

Professional service firms' risk profiles are changing due to the increased use of technology and tools such as artificial intelligence. Firms may encounter significant impacts on business models and client needs. While the additional complexity will reduce some risks, it is likely to create others.

Which pressures are changing risk profiles?

Risk is ubiquitous in today's uncertain world. The evolution and adoption of new technologies continues to add new complexities to professional service firms' risk profiles. It is reasonable to assert that organizations have less control over the range of risks facing them and that past data and experience are less valuable in risk analysis and assessment.

We are faced therefore, with a more ambiguous environment and a wider range of threats than risk functions may have traditionally addressed. For example, one prominent risk in many surveys is recruiting and retaining the right talent for today's competitive environment.

Changing risk management

The traditional understanding of risk implies the ability to identify, analyse and even quantify risks. Identified risks populate a risk register, where their effects and probability are charted, and a combined score signals the overall severity of the risk. This calculation may not reflect today's reality.

The digital economy brings new risks that are not yet be fully understood. They may not lend themselves to the traditional process of risk identification and analysis. They are more complex, interconnected and involve third parties – regulators included.

Understanding risk: complexity and control

Here are three categories of risk judged by their levels of complexity:

- **Simple risks** – capable of being controlled and treated. Causes and effects are clear (compliance, regulatory, some privacy and data protection issues).
- **Complex risks** – need broader expertise to assess and evaluate: may contain variables and have unknown effects (cyber security breach, some engagement failures, technology changes)
- **Ambiguous risks** – complex, dynamic and changing, multiple stakeholders (reputation, disruptive competition, regulatory changes, unexpected external shocks)

Many of today's risks have complex, ambiguous and dynamic characteristics.

Moving forward: technology and changing risks

The new and emerging risks identified in Aon's most recent risk management survey of professional firms showed some genuine shifts

- A movement towards concerns about external factors and away from traditional risks
- Risks emerging from adoption of technology, cyber, disruption and competition were more prominent

The risks associated with technology included:

- Disruption to business models and competition
- Cyber threats
- Regulatory changes and heightened scrutiny
- More complex Business Interruption loss scenarios

Understanding the risks associated with employing technology remains a challenge. Lessons from other areas of risk management show that the interaction between humans and technology is at the core of many incidents. So-called 'human errors' often occur in complex risk environments. In some instances, the wrong judgement is applied. A system failure at a UK bank was widely reported as a technology issue at the time of the incident. It subsequently emerged that in fact decisions were made at the board level that prioritised the speed of transition at the expense of technical thoroughness.

Cyber is a complex and ambiguous risk with a large human element. This is the area of systems thinking where the relationships between people, processes, procedures and technology must be considered to ensure a comprehensive approach to risk management.

The cyber challenge

Increased levels of defence are required to address changes in technology use and consequent risk complexity. Serious or new threats include more invasive malware, executing cloud security responsibility, mobile attacks, ransomware and social engineering. Maintaining current protections and combating the ingenuity of attackers are not straightforward challenges. Selecting the right technology is a risk that appears in some registers on both the operational and security fronts.

Even organizations with a full stack of technical protections and robust processes have fallen victim to attacks. Clients and the media will be unforgiving if a data loss incident occurs, and severe reputation consequences may follow.

The level of protection and budgets remain challenging for management. An organization's risk tolerance and appetite come into the equation. Breach response costs are increasing, and additional costs are being added in the recovery phase, after the initial response and short-term continuity phases.

Here are some lessons in the cyber area:

1. Think about what could go wrong – root causes and consequences
2. Define proportionate responses and share them with business owners
3. Threat intelligence: learn from others to assess your vulnerability
4. Be prepared if things go wrong
5. Business risks need an inter-disciplinary response
6. Insurance can provide considerable value add

These lessons are applicable across all risks, but additional responses may be necessary.

How can risk management respond?

Organizational resilience is gaining ground as a concept to manage complex risks. Resilience includes examining the risk implications and responses of new practice areas, the adoption of technology, privacy and data loss, alliances and collaboration, political and regulatory risks and reputation.

Resilience allows an organisation to bounce back from adversity. It requires examination of root causes and outcomes, business continuity management and scenario planning. Risk leadership operates at a strategic level examining the future, and the wide range of threats to the business. Importantly this could include consideration of the composition of the future workforce.

A resilient organisation can deliver on the revenue and efficiency gains promised by new technologies. Internal functions are aligned, and certain features will be in place:

- **A risk radar** that articulates issues and provides an early warning system
- **Crisis management** is ready to be activated at pre-determined trigger points
- **Lessons from past experiences**, near misses and peer incidents are absorbed and lessons applied
- **A specific resilience agenda** is created and specifically is designed to protect reputation

In summary, risk governance must adapt to the new threats, methods of working and the new skill sets required. The degree of change to existing practices will be dependent upon the technologies being employed and the business issues being solved. Decisions may be less clear and the risk analysis more complex.

If you'd like to discuss any of the issues raised in this article, please contact **Keith Tracey**.