Risk Management in the Digital Age

Author: **Randy Sadler, *CIC Services***
Published: **March 23, 2022, *Treasury & Risk (ALM Publications)***

The business landscape has drastically changed in the past two years, as the pandemic fast-tracked technological advances. According to a McKinsey Global Survey, companies have accelerated the share of digital or digitally enabled products in their portfolios by a whopping seven years since Covid-19 became a global phenomenon. They are leveraging emerging technologies in areas such as cloud computing, cybersecurity, artificial intelligence (AI), telehealth, tools supporting ecentralized or remote workforces, and robotics.

So far in 2022, the digital economy has only continued to grow. IDC projects that, by the end of this year, 65 percent of global GDP will be digitalized, with nearly $7 trillion in investments injected into the IT sector through 2023.

What does this trend mean for corporate risk and treasury teams? The financial fallout from technological risks can be substantial. Corporate treasury and risk professionals must make a concerted effort, today, to understand and prepare for the ways in which the emerging technologies their companies are adopting should impact their organizational risk management.

Technological Advances Can Open Businesses to Lawsuits

In the case of telemedicine, telecommunications and information technologies are now enabling clinical healthcare to be performed at a distance. Many medical practices took advantage of this option during the pandemic, to continue operations with lower risk to both patients and providers.

This approach offered convenience and helped healthcare facilities sustain revenue levels during a difficult time, but it wasn't without drawbacks. In Hageseth v. Superior Court, a Colorado psychiatrist who prescribed medication based on a questionnaire, rather than assessing the patient's needs by meeting with him, was sued for malpractice. This example demonstrates that although telemedicine is practical, it also introduces practitioners to new exposures around misdiagnosis and malpractice. Telehealth businesses also face new regulatory risks and privacy and consent concerns.

Businesses in nearly every industry face these types of threats. Consider the automotive industry, for instance, whose manufacturers continue to unveil self-driving cars. In 2020, an incident involving an Uber self-driving car led to the death of a pedestrian. Although Uber was not held criminally liable for the fatality, the company did reach a legal settlement with the victim's family.

The Uber incident sheds light on the complex nature of liability in relation to artificial intelligence. When AI fails to address safety measures within a driverless car, or medical software AI fails to correctly diagnose a patient, who is legally responsible? The courts are in the early days of sorting out such questions. But as AI technology becomes more widely used and is incorporated into more and more aspects of everyday life, an increase in AI-related disputes will be seen in the coming years.

Potential Hazards and Risks in Robotics

Leveraging robotics to automate rote tasks—particularly in manufacturing—provides not only cost-savings benefits, but also betterquality and more consistent products, increased worker productivity, and reduced labor costs. However, relying on robotics can also introduce an assortment of new risks.

Like other technological advances, industrial robots can create concerns for human safety. Another significant issue is that mechanical failures may significantly impede operations. According to Erik Brynjolfsson, director of Stanford University's Digital Economy Lab, experimentation in robotics can lead to big mistakes as companies test products and push concepts. Boeing, for example, abandoned its costly and ambitious investment in robots for the 777 assembly line, reverting back to a more traditional production process to improve operational reliability. When robots fail to work as expected, the business may face a myriad of risks in terms of human safety, damaged products, and business interruption.

Cybercrime Continues to Escalate

It's no wonder that the frequency of cyberattacks nearly doubled between 2019 and 2021, according to a report from Cybersecurity Ventures. Technological advances enabled companies to respond to the pandemic by allowing entire teams to work remotely. This model has obvious benefits, and it enabled many companies to survive in the era of Covid-19.

At the same time, widespread adoption of remote work increased companies' potential exposure to cyberthreats. Businesses today are primarily vulnerable to attacks that hinge on human error. Employees might work with sensitive data while on public Wi-Fi, fail to sufficiently protect their various passwords, forget to back up important data, fall victim to phishing scams, download unapproved software, or connect to the corporate network using personal devices that are unsecured. All these risks might explain why a recent report by Forrester found that 74 percent of companies attribute recent cyberattacks to vulnerabilities in technology put in place during the pandemic.

(Continued)

How to Harden Corporate Defenses

Yet, as technological advances impact businesses in every industry and across the globe, many remain unprepared to manage and mitigate the associated risks. A 2021 report by Embroker found that most small and midsize enterprises are unprepared for the modern risks most likely to face their businesses.

As 2022 unfolds, corporate risk and treasury teams need to incorporate the implications of emerging technologies into their evaluations of corporate risk. It's helpful to begin by taking the following steps:

1. Conduct a technological risk assessment to determine which risks your business is most likely to face. Calculate both the probability and potential impact of each significant risk.

2. Review the company's insurance policies to pinpoint which of these risks are covered and where the company may be uninsured or underinsured for specific risks.

3. Analyze your organization's security measures in each area. Ensure that proper procedures are in place to mitigate the technological risks that pose the greatest threat to the business.

4. Implement a disaster recovery and business continuity plan, if the business doesn't yet have one. Conversely, if a disaster recovery plan is already in place, review it for needed updates.

Walking through these four steps for each technological risk your organization may face will place your business on better footing should the worst-case scenario unfold. You may find that your company needs to revise risk mitigation and planning processes for specific types of risks.

You may also find that those activities, alone, aren't enough to protect your business. For example, insurance policies that cover cybercrime losses often have exclusions. They may not pay claims stemming from human error—which can be devastating for businesses, as a majority of cyberattacks result from vulnerabilities created by employee mistakes. Also, the complex and ever-changing nature of technology means that even the best-laid plans can fail.

In these types of cases, companies may want to consider captive insurance. A report by Aon found that cyber risk coverage in captives has increased 650 percent over the past five years. A benefit of this approach in the rapidly changing technology landscape is that a company which owns its insurer can write broader policies that cover a wider array of technological threats and better ensure the payment of claims.

Technology will undoubtedly continue to progress, and companies will be expected to continue embracing new and emerging innovations. That means risk management teams will continue to navigate uncharted territory. But with the right measures in place, they can minimize the financial repercussions of technology related loss events.

RANDY SADLER started his career in risk management as an officer in the U.S. Army, where he was responsible for the training and safety of hundreds of soldiers and over 150 wheeled and tracked vehicles. He graduated from the U.S. Military Academy at West Point with a Bachelor of Science degree in International and Strategic History with a focus on U.S. – Chinese Relations in the 20th century. He has been a Principal with CIC Services, LLC for 7 years and consults directly with business owners, CEOs and CFOs in the formation of captive insurance programs for their respective businesses.

CIC Services, LLC manages over 100 captives.