Scoping a Cyber Catastrophe

Understanding the Societal Impact of the Fourth Industrial Revolution and The Role of Insurance

CyberCube

www.cybcube.com

The global economy is racing to digitize its service and product offerings and this "Fourth Industrial Revolution" has far-reaching implications for society. In light of the growing dependence on technology through the Internet of Things (IoT), all aspects of society are under greater pressure to focus on risk management, mitigation and transfer as the global economy evolves to support the technological revolution.

With this exponential rise in the connected economy, there is huge opportunity for both innovation, but also for exploitation.

Our digital future will be determined by permutations of various technological, political, business, cultural, military and societal developments that will reshape the economy, society and therefore risk management. Each of these sectors has a duty to invest in understanding both the opportunities and risks presented by digital risk, and act within their communities to influence the impact that the Fourth Industrial Revolution could have on society.

For centuries, the insurance sector has played a pivotal role in unlocking the economic potential of technical innovation, by providing crucial financial support for organizations to transfer risk that can not be managed on balance sheets. The authors of this paper believe that internet-connected technologies is a prime opportunity for the insurance sector to be at the forefront of understanding the risks, setting standards for controlled growth and assuming financial risks on its balance sheets where needed.

An estimated

$1.25 trillion

was spent on digital transformation globally in 2019

Imagining Scenarios

However, understanding risk starts with the individual organizations forming a robust view of the potential impact of technology on their business.

Scenario-building is an important tool in helping organizations to develop their own risk tolerance and strategic direction with technology. The use of scenarios to explore uncertainty requires "disciplined imagination", however, rather than straying into the realm of science fiction.

The use of models to consider realistic cyber attack scenarios and to quantify the financial loss from those events is a useful tool to assess risk and make informed decisions.

An estimated $1.25 trillion was spent on digital transformation globally in 2019. That number is forecasted to reach $1.97 trillion in global spending on digital transformation of businesses in 2022, according to the International Data Corporation (IDC). Growth in every industry will be driven by digitally-enhanced offerings, operations, and relationships.

Behavioural science, data science and technology provide enormous potential benefits to society. However, contextual awareness of the cyber environment in which businesses operate is essential with a breach potentially having negative repercussions on society.

For example, loss of service and disruption to supply chains through system downtime

is one possible consequence. An unsecured hyper-connected system could represent an opportunity for a criminal actor to disrupt society. The NotPetya cyber event in 2017, although essentially an attack targeting business in the Ukraine, was one such highly disruptive episode. In this instance, there were no geographical boundaries to the effect of the attack, with the internal networks infected within multi-nationals including shipping company Maersk, logistics group Fedex and pharmaceutical conglomerate Merck.

As these digital onslaughts increase in sophistication and attack surfaces become larger, these types of breaches are likely to affect a more diverse base. The use of personal data (not just financial but also, geographic and social) will quickly move up the political and socio-economic agenda as society becomes more reliant on systems that share more personal information, including locations. That data could be stolen and used for nefarious purposes, with geo-locational movement and routines potentially being tracked, monitored and exploited.

As 5G powers more access to critical infrastructure and to associated online services, a cyber attack on a network could have a huge knock-on effect, not just in terms of financial impact but also on people's everyday lives. Speed is increasingly key to the cyber criminals' offensive strategy and, as 5G becomes ubiquitous, larger data packages will facilitate easier and more impactful attack campaigns. Technology companies and Telcos will need to get ahead of these potential cyber attack challenges prior to 5G rollout across the world's smart cities.

Potential Attack Narratives
National Infrastructure

Malicious cyber actors can leverage IoT vulnerabilities to target critical infrastructure facilities, such as power plants, national railways and local underground systems or other forms of public transport. Cyber attacks could cut off the supply of electricity to hospitals, schools, factories and homes affecting all walks of life.

The WannaCry outbreak in 2017 demonstrated the impact of an infrastructure attack on a public service. It had widespread consequences, shutting down computers in more than 80 NHS organisations in England alone. NHS England estimated over 19,000 appointments were cancelled in total.

In addition, there is the prospect of an increasing impact of geopolitics on cyber risk landscape. For example, nation state-backed attacks could be aimed at high-profile events such as the Tokyo Olympics.

Potential Attack Narratives
Transportation Infrastructure Attack

Transport infrastructure vulnerabilities are coming under the microscope as railway companies digitize their services. Trains - with no drivers - that are run by sensors may fall victim to a rail incident. For example, malicious state actors or terrorists could take advantage of cyber attacks to create crowd surges to popular locations, such as a train station, or a voting booth during an election.

Voting systems have already been manipulated as demonstrated by the 2014 presidential election in Ukraine. Hackers infiltrated workstations of the Central Election Committee and destroyed various files, including those necessary for vote tabulation.

There were several attempts to compromise the election, including an effort from the cyber espionage group APT Dragonfly, which is reportedly associated with Russian actors. Shortly before the first round of the presidential elections on 31 March, authorities discovered an attack against the Vybory system consisting of almost 100 phishing emails containing previously unknown, unique malware.

This is a concern at a nation state level but in terms of the wider society, it is now clear that in the future, as vertical markets become digitised and hyper-connected, risk management professionals will need access to tools and skillsets that mitigate these risks.

Resilient Organizations

As intangible and tangible items become hyperconnected, the implications of failing to get security and privacy right have much bigger consequences than they have had in the past. The outcomes will not just affect technology departments and their operations, but could have a significant detrimental effect on society.

A holistic, enterprise-wide programme for managing cyber risk is fundamental for companies today and they need to think differently and more proactively about cyber security and resilience in their organisations.

Rather than focusing on cyber as an IT project, it is important to consider how risks (both technological and people-based) interconnect across an entire business structure. A cyber resilience programme should focus on the following areas:

Strategy & Culture A comprehensive and integrated cyber resilience programme should start (not end) with business culture and people. Questions such as "what kind of business are we?" and "how much risk should we be taking?" (preferred risk tolerance) should be asked and agreed at board level. This approach will ensure that other elements of the programme such as communication strategy, ownership, incentives/penalties and governance can be properly aligned.

Organization & Governance Having determined a clear and culturally aligned cyber resilience strategy, attention should be given to how a continuous improvement programme should be structured and governed. Of particular importance here are elements such as organisational structure. Roles and responsibility and management reporting are key.

Policy The definition of policy and controls that are aligned to strategic objectives and overarching governance should be carefully constructed and take into account how best to execute against programme objectives. Regulatory compliance, working best practices, industry standards, as well as enforcement and monitoring can be defined here.

Process One of the major shortfalls of many cyber resilience initiatives is inconsistent implementation and an inability to automate manually-intensive technical processes. Lack of standard processes (workflows) has led to some of the most significant business outages in recent years. Standardisation in this area, followed by appropriate automation is vital in building a cyber resilience programme that is fit for purpose. Definition of change control and breach response process should be given particular attention here.

Technology Companies are using a portfolio of security tools such as defence and in-depth artificial intelligence (AI) to prevent cyber attacks. However, a rush to take on a variety of new security products can act as a distraction from preparing for a cyber breach. Ironically, security tools are part of the problem as business can find they have dozens of software products which are not interconnected or prioritised. A move towards security platforms, as opposed to adding even more discreet tools, is at least part of the solution. Technologies should be carefully assessed and chosen based on the other element of a cyber resilience programme rather than on industry trends and on what happens to be fashionable at any given time.

Of course, the cyber resilience programme should be implemented with continuous improvement in mind. Each element of the programme model should be constantly reviewed and tuned to changing business objectives, market conditions and risk landscapes.

The World Economic Forum has also published a set of principles for cyber resilience. These include a company's board as a whole taking ultimate responsibility for oversight of cyber risk and resilience (see Appendix).

CyberCube and the World Economic Forum

The threat of cyberattacks was highlighted in the World Economic Forum's (WEF) Global Risks Report for 2019. It stated that cyber attacks pose risks to critical infrastructure, prompting countries to strengthen their screening of cross-border partnerships on national security grounds.

In July 2019, CyberCube, was selected among hundreds of candidates as one of the WEF's "Technology Pioneers." Technology Pioneers are early to growth-stage companies from around the world that are involved in the design, development, and deployment of new technologies and innovations, and are poised to have a significant impact on business and society.

CyberCube creates technology and analytics to help society better understand the financial impact of one of the most important risks of the 21st Century. Our data-driven analytics empower the insurance industry to unlock the financial potential of technological change for millions of businesses.

We look forward to contributing to the WEF dialogues on this challenge.

The Role of Insurance in Unlocking Digital Potential

As the global economy eagerly embraces technological change and demands a constant connection to the world, society and its relationship to technology is redefining the nature of risk. The nature of perils is changing, with digital risk becoming a peril warranting specific and immediate attention.

For centuries, the insurance sector has played a pivotal role in unlocking the economic potential of technical innovation, by providing crucial financial support for organizations to transfer risk that can not be managed on balance sheets.

One of the important functions of insurance is to act as a driver to modify behaviors and incentivize certain outcomes. Historically, insurance has driven improvements in building regulations, safety standards against natural catastrophes, car safety and liability and standards in product design.

One of the fundamental principals of insurance is for the insured entity to act as a "prudent uninsured", or as if no cover existed. There is an obligation on organizations that are developing, or applying new technology, to adopt this principal. However, for risks that are transferred to the insurance sector, the insurance industry's role in setting cybersecurity standards, incentivising secure and responsible innovation, and providing meaningful risk transfer products is crucial today.

There are some practical ways in which the insurance sector could fulfill this role. These include:

- Applying a financial cost to cybersecurity best practice, through the premiums it charges for risk transfer. By asking the right questions and incentivizing best cyber hygiene with premium discounts or enhanced coverage, insurers can help promote the adoption of good practice. This is already the case, for example, in property insurance, where premiums are lower for facilities with fire sprinkler systems and motion sensors.
- By its nature, the insurance sector pools risk across multiple companies, geographies and industries. Shared data empowers the insurance industry to drive loss prevention best practice. Insurers will help firms reduce their losses by providing insight from claims and near misses across their client base. Pooling information is of particular value for cyber risk, because cyber is a new risk and incidents are often unreported.

The Role of Insurance in Unlocking Digital Potential

- While large corporations may rely on their own internal resources to mitigate the effects of a breach, most SMEs do not have these resources. They often turn to external vendors for remediation following a cyberattack. Insurers could offer access to approved vendors providing not only professional remediation but also tools to improve resilience against future attacks.
- Developing a standardized reference set of scenarios can project the size and scope of cyber catastrophe events, using financial modeling tools. With multiple stakeholders working on a shared view of risk, collaboration across public and private sectors on innovation and resilience could be enhanced.
- The insurance sector and government are in a position to jointly enforce minimum levels of cyber resilience. Standards, such as the UK Cyber Essentials, or the US's National Institute of Standards and Technology (NIST) Cybersecurity Framework already exist. As with compulsory general liability, or motor insurance coverage today, governments could mandate the purchase of cyber insurance policies that meet minimum standards.

Given the risks attributable to cyber can never be reduced to zero, insurance provides a way to transfer some of the residual cyber risk that is inevitable for any modern organization. For a company spending $20 million on cyber security, it is an appropriate question to ask whether that company is best served spending an incremental $1 million on more cyber security or on cyber insurance when a holistic risk management lens is considered.

Appendix
WEF Principles for Cyber Resilience

Principle 1 Responsibility for cyber resilience
The board as a whole takes ultimate responsibility for oversight of cyber risk and resilience. The board may delegate primary oversight activity to an existing committee (e.g. risk committee) or new committee (e.g. cyber resilience committee).

Principle 2 Command of the subject
Board members receive cyber resilience orientation upon joining the board and are regularly updated on recent threats and trends – with advice and assistance from independent external experts being available as requested.

Principle 3 Accountable officer
The board ensures that one corporate officer is accountable for reporting on the organization's capability to manage cyber resilience and progress in implementing cyber resilience goals. The board ensures that this officer has regular board access, sufficient authority, command of the subject matter, experience and resources to fulfil these duties.

Principle 4 Integration of cyber resilience
The board ensures that management integrates cyber resilience and cyber risk assessment into overall business strategy and into enterprise-wide risk management, as well as budgeting and resource allocation.

Principle 5 Risk appetite
The board annually defines and quantifies business risk tolerance relative to cyber resilience and ensures that this is consistent with corporate strategy and risk appetite. The board is advised on both current and future risk exposure as well as regulatory requirements and industry/societal benchmarks for risk appetite.

Principle 6 Risk assessment and reporting
The board holds management accountable for reporting a quantified and understandable assessment of cyber risks, threats and events as a standing agenda item during board meetings. It validates these assessments with its own strategic risk assessment using the Board Cyber Risk Framework.

Principle 7 Resilience plans
The board ensures that management supports the officer accountable for cyber resilience by the creation, implementation, testing and ongoing improvement of cyber resilience plans, which are appropriately harmonized across the business. It requires the officer in charge to monitor performance and to regularly report to the board.

Principle 8 Community
The board encourages management to collaborate with other stakeholders, as relevant and appropriate, in order to ensure systemic cyber resilience.

Principle 9 Review
The board ensures that a formal, independent cyber resilience review of the organization is carried out annually.

Principle 10 Effectiveness
The board periodically reviews its own performance in the implementation of these principles or seeks independent advice for continuous improvement.

Source: Advancing Cyber Resilience Principles and Tools for Boards, Jan 2017

Authors

Darren Thomson, Head of Cyber Security Strategy

Rebecca Bole, Head of Industry Engagement

Yvette Essen, Head of Research & Communications

United States

CyberCube Analytics
58 Maiden Lane
3rd Floor
San Francisco CA94108

Email: info@cybcube.com

United Kingdom

CyberCube Analytics
51 Eastcheap
1st floor
London EC3M 1JP

Estonia

CyberCube Analytics
Metro Plaza
Viru Väljak 2
3rd floor
10111 Tallinn

www.cybcube.com