Uncertain insurance futures:

The importance of thinking beyond the horizon on digital risk

CyberCube

www.cybcube.com

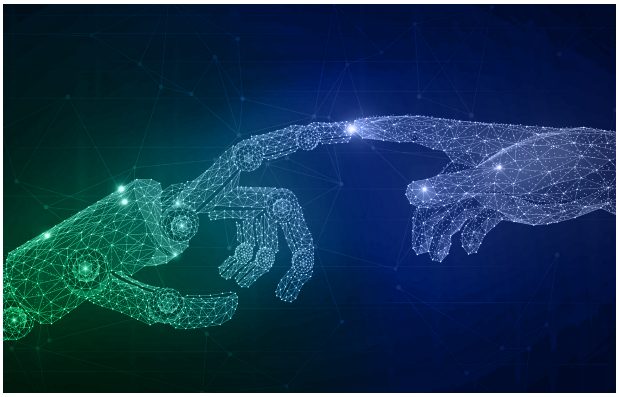
Executive Summary

Internet-connected technologies will fundamentally reshape risk in the 21st Century and in doing so they will fundamentally reshape the risk transfer industry.

Trends such as the exponential rise of data, the growing ubiquity of the internet of things, the automation of industries and the increased use of artificial intelligence are reshaping the economy and society. While it is tempting to extrapolate those trends and paint an inexorable march towards a digital future that is knowable today and is only a matter of time before we see it realized, the reality is a lot more uncertain.

> **We always overestimate the change that will occur in the next two years and underestimate the change that will occur in the next ten. Don't let yourself be lulled into inaction.**
>
> **Bill Gates**
> *Microsoft founder*

The Fourth Industrial Revolution (4IR) is creating exponential change, rather than linear. It is possible that misleadingly little will appear to change in the risk landscape over the coming two years. However, the ten-year time horizon could deliver a world that looks very different than that of today.



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.

This white paper builds on a series of workshops undertaken by the UC Berkeley CLTC, in association with the World Economic Forum (WEF) about how those uncertainties could lead to very different cybersecurity futures, applies an insurance lens to those futures and attempts to draw out what an uncertain digital future means for (re-)insurers today.

The only thing we know for certain is that the future of risk is indeed uncertain. This white paper is intended to provoke thought on what some of those uncertainties are for (re)insurers and what they can start doing today in the face of that uncertain digital future.

Exploring scenarios to inform strategy

Scenario-building is an important tool in helping organizations to develop their own strategic direction & priorities: starting from uncertainties in the contextual environment, and working inwards via the industry or transactional environment toward the organization's own strategic decisions.

The use of scenarios to explore uncertainty requires "disciplined imagination", however, rather than straying into the realm of science fiction.

The CLTC, WEF and CNA Institute applied its "**disciplined imagination" to cybersecurity, defining it as the 'master problem of the Internet era**".

The research (details can be found here https://www.cybcube.com/resources/uc-berkley-center-for-long-term-cybersecurity/) produced four initial scenarios which encompass divergent scenarios for the future of cybersecurity:

NEW WIGGLE ROOM:

Exploring multiple or imperfect identities

This is a world in which there is 'perfect information' and imperfect identity. The combination of omnipresent sensors and ubiquitous connectivity turns out to be a poisoned chalice. We now know too much—and know it too accurately—for societies to remain stable and people find ways to introduce new uncertainty by adopting multiple identities.

QUANTUM LEAP:
Encryption is broken, what does that mean for data security?
This is a world in which a few large governments attempt to control the proliferation of quantum computing technology. Non-proliferation fails, leaving re-shuffled geopolitical alliances and new centers of power. Quantum technologies fall into the hands of city consortia and deviant criminal networks.

TRUST US: Artificial Intelligence is advanced enough that people trust it. AI can, therefore, deceive us.
This is a world in which an AI-powered "SafetyNet" overwhelms security challenges & makes the digital world safe for big institutions. However, for most individuals, privacy is a distant memory and there is looming distrust of AI that is capable of explaining its own decision- making processes to humans and knows exactly what they want to hear.

BARLOW'S REVENGE:
Nation states no longer govern, ceding control to the private sector and criminal groups.
This is a world in which two nearly opposite grand bargains for digital security emerge. Some countries secure the internet within their borders by essentially nationalizing it; other governments cede all responsibility to corporations and the market. The balance of regulation and innovation that the digital world inhabited for the last 40 years is hollowed out.

These scenarios were created and refined over a series of 8 workshops in cities around the globe with leaders across industries.

CyberCube and the CLTC gathered a group of insurance strategists from major insurers and brokers to take the output from this work and put an insurance-specific lens on it. The group reflected on how much and how rapidly the nature of risk will change in 5-10 years and how that might impact the insurance and risk transfer industries.

Spectrums of uncertainty:

The insurance working group outlined the major macro-level uncertainties that could be instrumental in the 5-10 year timeframe. They then set out the range of uncertainty at each end of the scale:

DECISION MAKING

Humans in loop → Fully autonomous

JOB DISPLACEMENT

Gradual & incremental → Dramatic & fast

WEALTH CONCENTRATION

Less → More

DIGITAL TECHNOLOGY STANDARDS

Consolidating & open → Diverging & proprietary

LARGE DATA SETS

Assets → Burden, liability

AMBIENT TRUST

Lower → Higher

GROUP IDENTITIES & SOCIAL NETWORKS

Official, institutional, characterized by few "thick" ties → Tribes, self-identified, characterized by many "thin" ties

INDIVIDUAL AUTONOMY

Shrinking → Expanding

ATTACK VECTORS

Physical, with violent conflict dispersed → Digital, with violent conflict amplifying

Discussion and exploration of these uncertainties exposed the potential for many different worlds that we could be occupying in the near-future:

- Data allows almost infinite granularity in risk selection for insurance, with some sections of the economy and society unable to secure insurance.
- A Universal Basic Income may come into effect, taking the insurance of the many back to the State
- The 'risk pool' becomes too homogenous (with the best risks selected). This could put the fundamental concept of risk pooling in jeopardy
- Developments in technology and geopolitics lead to a fracturing of the globe and a "deglobalization" that leads to tremendous disadvantages for any global (re-)insurer seeking to provide coverage in all parts of the world
- A future where the economy becomes highly automated, digitized with expansive growth in artificial intelligence, robotics, and machines resulting in the insurance of algorithms become the pervasive line of insurance to cover
- Information is manipulated and imperfect, with trust at an all-time low: the insured does not trust the insurer to make appropriate risk decisions or pay claims
- A highly automated world where employment is rapidly displaced by internet-connected machines and risk becomes highly digitized but the catastrophic risks of those machines failing creates such immense losses the insurance industry struggles to provide sufficient capital to provide meaningful cover
- Individual or corporate liability may not exist, as all decisions are made by a few, powerful algorithms. All decisions are autonomous
- At the other end of the scale, large tech corporations fragment, and there is a possible future where society retrenches to the physical and analog, from the digital as a backlash against trends seen today, which intensify

It is important to note that none of the scenarios discussed were discrete or the 'end game', but could each occur incrementally and modularly in a continuum. Each was intended to provoke discussion and debate about highly uncertain futures, which was certainly the case from those participating in this workshop session.

How can the insurance industry act today, for an uncertain tomorrow?

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. The insurance industry is uniquely placed to continue this role with technological developments and the changing nature of risk in the coming years.

It is valuable to reflect on whether the insurance sector is a passive actor in the Fourth Industrial Revolution, or whether the sector is acting as an 'enabler' of technology by driving best-practices and sharing new risks as they appear.

In an uncertain future for the insurance industry, what should (re)insurers be doing today?

Participate in the cyber insurance market with a learning mindset that expands far beyond today's digital risk needs – Digital risk will transform almost all other lines of P&C insurance. Developing the capability to understand digital risk as an insurer in the future extends far beyond the need to provide "data breach insurance" today but becomes a peril that transverses all lines of insurance in the future (e.g., property, auto, D&O, product liability)

Recognize that regulation of internet technology has the potential to create major discontinuities – As technology risk transforms society, it will attract major regulatory attention, even if it takes cataclysmic events for politicians and regulators to take action. Any business model based on transferring technology risks needs to assume that technology companies are fundamentally vulnerable to invasive regulation that can fundamentally alter the risk (and risk transfer) landscape

Insurers must invest in new data and analytics capabilities, including data governance – The volumes of data required to understand cyber and digital risk are unlike anything that the insurance industry has experienced before. Not only do insurers need to invest in new capabilities to process and understand that data, but they also need to be mindful that there could be dramatic shifts in how that data is regulated and can be used

Develop localized approaches to digital risk, as well as global approaches – Digital risk provides an opportunity for global insurers to develop global capabilities, products, organization and information sharing. At the same time, it is important to be mindful of local variations in technology ecosystems (e.g., China and the US could conceivably have mutually exclusive ecosystems), consumer sentiments towards digital (e.g., privacy could be an overarching top of mind source of risk for some consumers and irrelevant to others) and regulation (e.g., widely different local, national or supra-national regulatory regimes may emerge)

Be mindful of unidentified technology aggregation in any new policy wording being drafted today – Sources of technology accumulation will increasingly show up across almost all lines of P&C insurance. It is not inconceivable that (re)insurers run the risk of an 'asbestos' moment where a technology event could cause a drag on industry financial results for a generation and therefore recognizing the potential for unknown unknowns is essential in policy design and wordings as well as designing new policies that address the new risks we face in the 21st Century

Insurance of digital risk should be a core component of any insurer's long-term planning: Cyber risk currently costs the economy at least $400B per year and that number could easily reach trillions of dollars and a substantial portion of global GDP in the decade ahead. Such enormous growth in new risk pools creates enormous (potentially even unparalleled) opportunity for the risk transfer industry to become more relevant in the generation ahead. The market opportunity is both too big to ignore and also large enough for (re)insurers to place bets on small segments of that market and still create very large and profitable businesses (without taking on what might be deemed 'uninsurable'). At the same time, the future of digital risk is so uncertain, it needs to be revisited regularly and subject to the kind of pressure testing of various future scenarios, which are unknowable today.

background to CyberCube's approach

CyberCube is dedicated to providing the cyber risk data and analytics needed by insurers to undertake controlled growth with emerging digital risks. Today, our cyber aggregation scenario modeling is used by our (re)insurance carrier customers, who represent around half of the global cyber insurance market, to understand the probability and severity of catastrophic events that could impact the balance sheets of insurers over the next 12 months. Over the long-term, our aspiration is to become the pre-eminent. data and analytics partner to the P&C insurance industry as cyber and digital risk reshapes almost all lines of insurance. For more information, **contact us at info@cybcube.com**.

CyberCube was appointed to the World Economic Forum's Technology Pioneers program in 2019. The World Economic Forum's 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. **https://www.weforum.org/communities/technology-pioneer**