THE ACCLAIM TIMES

Permit No 040/10/2017

Acclaim Insurance Brokers Pte Ltd

- CYBER SECURITY -

The Biggest Challenge in the Digital Age

Mr Peter Hacker, Acclaim's exclusive cyber consultant for the Asian region, and internationally recognized cyber security, InsurTech opinion leader, author and multilingual public speaker shares his thoughts on Digital Disruption and Cyber Risks.

Innovation and Global Impacts

We live in an era of change where technology and society are evolving faster than businesses can naturally adapt. This will set the stage for a new generation of business models with unparalleled intangible risks and opportunities, growing a new era of leadership charging behind a mantra of adapt or die. With this heightened utilization of automation and digitalization, it means that we need to equip ourselves with the right tools, solutions and skills to remain relevant.

Technology cycles are accelerating exponentially where digital disruption is certain. The rules of engagement in business are being redrafted. Digital disruption is indeed not just a concept. A lot of opportunities will present itself if we find a way to capitalize on disruptions, attract talent from outside and offer an organizational culture that accepts failure and change. Within the next five years, we will see things that are purely fictional today becoming a reality. We will see Disruptive Technologies such as Artificial Intelligence, Blockchain, and the Internet of Things having a massive impact on risk and business models. Everything is moving to the Cloud - Blockchain, or Digital Currency.

Risks are becoming more volatile and intangible

The rapid rate at which technology is advancing presents growing challenges for corporations, regulators, legal systems, insurers and brokers. Often emerging disruptive technology e.g. artificial intelligence, drones, autonomous robots, self-driving vehicles, 3-D printer, Internet of Things is advancing so rapidly that governments and regulators cannot foresee and react, resulting in uncertainties, liabilities, intellectual property or thorny security, data privacy and intangible assets (brand/reputation) issues.

With the broader acceptance of disruptive technologies, it is important to note that the aggregation of risk will further increase and there will be a significant shift from tangible exposures into intangible ones. Market capitalizations will be heavily driven by intangible assets such as data, reputation, brand, Intellectual Property, and the relationship between customers and suppliers. These will increase the magnitude of intangible risks from an abstract rarely relevant risk to a real threat in almost every sector. These developments will require a new way of identifying, evaluating, reserving risk and broader diversified risk skill sets.

Exponential Cyber Risks and what lays ahead

Technology is redefining how we live in today's fast paced world. Digitalisation is becoming the order of the day, disrupting the conventional business methods and strategies at an unprecedented pace. Risks are changing globally thanks to digital trends such as the acceptance of online commerce, the rise of social media, and the proliferation of mobile devices.

One crucial risk area to businesses we have seen in recent times is that of cybersecurity. The global cost of cybercrime is predicted to reach £4.9 trillion annually by 2021 and new cybersecurity trends are emerging. Recent attacks such as the WannaCry in May, the attacks on PetroChina, Qihoo 360, Parliament, or the Petya ransomware attack on WPP, Mondelez, Maersk, Merck in late June have brought this further in to the forefront. WannaCry and Petya have taught the world that it is no longer a question of whether system can be hacked or not but ensuring tight cyber security protocol in detecting potential hacks if it happens.

ACCLAIM

Without a doubt, there will be many more 'landmines' in 'people's inboxes' and 'company's systems' waiting to emerge and present itself. To fight future threats, society must develop the next generation of cyber skills and bespoke risk transfer and advisory solutions to address or mitigate these emerging threats.

There will be more need for cyber security investments (detection, response and control) and smart enterprise risk management including insurance (identification, quantification and risk transfer). We all need to gear up for these developments. The importance of recognizing such trends got reiterated with the latest incident in Malaysia on October 31st. Malaysia is investigating an alleged attempt to sell the data of more than 46 million mobile phone subscribers online.

For the insurance industry, these developments will offer vast opportunities for product development, process efficiencies, and much lower transaction cost. By the same token, it will also present massive security, regulatory, silent risk transfer, broad enterprise risk management challenges and a potential to create broader earnings and capital hits. Damages of more than USD 300 million are unfortunately a reality and go beyond what even large companies can handle without proper Cyber Security and Enterprise Risk Strategies. Without any doubt, **Cyber Security and Cyber Risk are a fundamental Board topic.**

Gearing up for the time

The era of intangible risks, disruptive automation and digitalization are fast approaching, and we need to be prepared to maximize these changes to a significant effect. Foreseeing such change is no longer something that can be left to organizations, enterprises and corporations risks, legal and IT security teams. It is fundamental to understand and appreciate both risks and opportunities across individual organizations, and in particular at board level. These technologies have the great potential to continue connecting billions of people to the Worldwide Web, drastically improve the efficiency of businesses and organizations and help regenerate the natural environment through better asset and risk management. These new technologies will impact all disciplines, economies and industries to even challenge our ideas about what it means to be human.

The philosopher Marshall McLuhan once said: 'It is the framework which changes with each new technology and not just the picture within the frame.'

Data mining and analysis is King

Technological trends are bringing about change at an unprecedented rate. It is estimated that nearly 50% of subject knowledge acquired by a student in the first year of a four year technical degree will be outdated by the time the student graduates. 65% of students entering primary school today will end up working in a job that does not exist today. We foresee the requirements of hundreds of new skills needed and there will be massive demand for big data resulting in a call for data analysts, scientists and in the context the insurance industry, bespoke insurance advisory and risk transfer. In China, there is a saying: 'Ask the children if you want to know what is going on'. Data mining and analysis are more important than any other digital technology. There should be a strong endeavour and desire to connect the dots beyond applications, big data, customer engagement or even social media. Needless to say, we must become truly mobile with our business model. Mobile devices are becoming our external brains, where everything is being connected including our environment.

95% of the Internet will become mobile within the next five years. The growth potential will bring about some fundamental structural changes helping better identify, quantify, select and measure risks. It is our time to analyse, sort our value proposition and stay consistently ahead.

ACCLAIM

Technology will aid better understanding of risks at Board level

It is fair to assume that Disruptive Technology will change risk perception fundamentally and reiterate the importance of Enterprise Risk Management at the Board Level. Despite digital trends, customers will always require risk transfer and new solutions. The increasing scale of emerging intangible cyber exposures and the potential liabilities and loss of profit from new legislation (data directives/regulations) will open the floodgate for bigger and frequent losses.

Some might claim, Cyber Security Risk is not a new major threat to businesses. However, thriving globalization, unprecedented interconnectivity and commercialization are now unleashing massive new, opportunities and unknown risks on a scale we have never seen before. Directors cannot afford to be blindsided and be confronted with fiduciary and/or Directors and Officers claims. Whilst there is no pre-set standards and guidelines for boards and risk stakeholders to think about digitalization and its implication on Cyber Security, there are some fundamental questions to consider:

--- What risks and attacks are most likely to occur and what would the potential adverse impacts be?
--- What are targeted (systems, processes, data) and most important and how?
--- What are the different legal data privacy environments a company is operating in?
--- Where do we hold, control, process data, and how can it be protected?
--- How do we stress-test our readiness across the company and in particular at board level?
--- Does top management thoroughly understand its fiduciary duties?
--- Do you have appropriate capacities, capabilities and the right strategy in place to defend strategically and operationally against such attacks?
--- What are the recovery capacities, what is most valuable and what is most vulnerable?

Cyber Security and related intangible risks such as Intellectual Property, Reputational or Branding Risk are rather abstract - until an incident occurs. Consequently, we need to think like a hacker, then ‘only a hacker can beat a hacker.’ Ethical hacking, governance and artificial intelligence based risk simulation approach (‘red-teaming’) at the Board level is a powerful trinity to achieve a tailor made of client understanding, risk alignment and enterprise risk structure.

Conclusion

Bespoke Cyber Insurance represents both an invaluable risk transfer mechanism and opportunity to organizations. Our ability to address such emerging risks needs to be sustainable and proactive as it might well make the difference between the sustained success of our industry, the loss of capital and ultimate relevance in the face of new and much better equipped market entrants.

Mike Tyson, former world heavyweight boxing champion once said: ‘Everyone has a plan until they get punched in the face’.

We can’t ignore the inevitable, and take the "wait and see" approach. Therefore, monitor vigilantly these emerging technologies, watch what competitors are doing and start devising a plan towards the implementation of these new technologies whilst identifying, quantifying, transferring and controlling intangible cyber risks across the company.

In some cases, this will require industry-wide collaboration, potentially capital markets solutions and government support. Let us not forget, intangible risks (including cyber) are rather unique, potentially global, fully man-made, that is highly severe and happens frequently in the worst case. Individual major risks and portfolio aggregation need to be seen as marathon challenges and not a sprint. It is a matter of time until regulators and rating agencies will want to get answers on risk aggregation, silent exposures, reserving and capital at risk. We better have some detailed and ring-fenced answers, otherwise, we will have ‘our Mike Tyson moment’.

Acclaim's inaugural Cyber Security Workshop - Understanding Cyber Risk

Acclaim organized its inaugural Cyber Security Workshop on 28th August 2017 for some of our clients. This workshop was conducted by our exclusive Cyber consultant, Mr Peter Hacker. The 2 half day workshops were held in Amara Hotel and was structured to put into perspective that addressing cyber risks is an Enterprise Risk Management (ERM) practice with insurance as but a part of the overall approach to cyber risk mitigation.

Photo taken during the cyber security workshop.

The workshop saw the senior management team of clients representing various industries like financial institutions, commercial, manufacturing, key infrastructure operators/owners, Oil & Gas, retail, commodities, not-for-profit organizations and healthcare, being actively engaged in discussions on issues ranging from Personal Data Protection Act to action points which can be utilized in reviewing their organization's overall cyber risk profile.

Peter conducted a brief simulation of a cyberattack which allow clients to understand the potential liabilities arising from a cyber breach and he further expounded on the tools and processes which an organisation can look to engage in determining and formulating an effective cyber risk management practice.

We conducted a post evaluation of the workshop with our clients and feedbacks we received included:

1. Deeper understanding of what is really meant by "Cyber" in the context of a business operation, where the loss suffered is usually not physical but rather the loss of intangible assets, e.g. reputation, goodwill, confidence, intellectual property, etc.
2. Greater appreciation of the potential liabilities arising from cyber issues.
3. Clarity in terms of coverage and exclusions under a typical Cyber policy.
4. Action points which can be used in an organization in assisting to determine its cyber exposures.

Photo taken during the cyber security workshop.

Given the rising frequency and threat of cyberattacks, Acclaim firmly believes that this is an area of ERM which warrants evermore increasing attention and vigilance. To this end, Acclaim maintain ourselves as our clients' outsourced risk management function and as such will continue to engage with our clients on this important aspect of their risk landscape through similar forums and direct engagements.

Many clients provided feedbacks on the practicality of the workshop, which is not insurance-centric, and the pragmatic analysis of the issues raised during the workshop with ERM as the overarching principle in addressing cyber risk.

For more information or on your insurance needs – please contact us at
Acclaim Insurance Brokers Pte Ltd
|T| +65 6225 5880 |F|+65 6224 1736 |E| admin@acclaim.com.sg
|W| www.acclaim.com.sg

A Member of the:
|Asia Australasia Alliance||Assurex Global||Brokerslink Global|GBN Worldwide|
Presence in more than 140 countries with over 500 offices worldwide

ACCLAIM