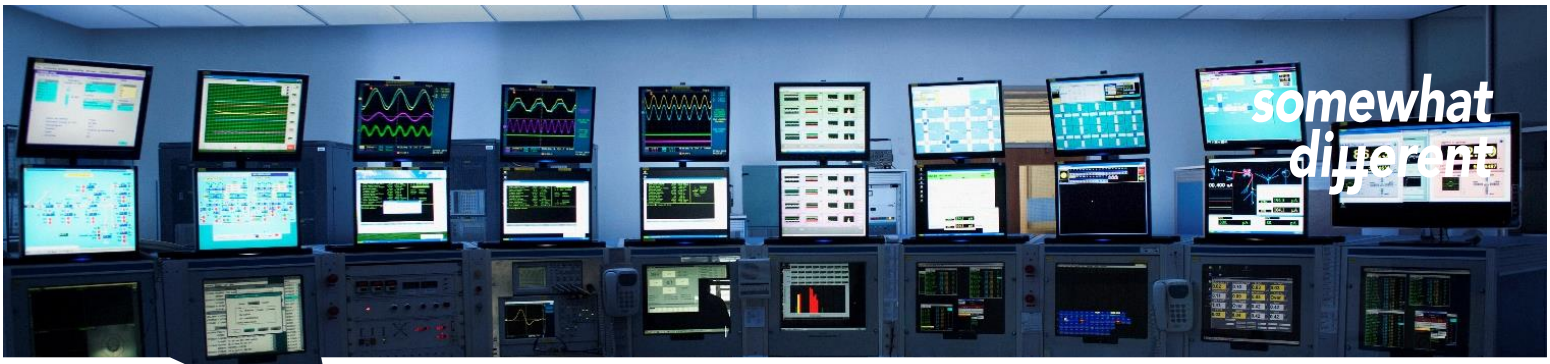

Digitalisation and interconnection is increasingly affecting the value creation of the global economy. This enables innovations and technology advances but also endangers operational risks of being amplified by cyber events.

Cyber Risks

The rapid advances in information technology over the past decade have introduced an entirely new set of risk exposures to companies that are increasingly dependent on information technology. In 1997, the first cyber risk insurance products began to emerge as carriers started identifying gaps in traditional property and general liability insurance products. Standalone network risk programmes offering affirmative first and third party coverage addressed threats posed by computer cybercrime, malware, and potential liability arising out of information security breaches.

We have come a long way since 1997. Global cybercrime has reached such a high level of sophistication that it represents a mature global business sector, which is continually innovating and getting more efficient. In 2017, a widespread use of nation-state calibre attack methods by criminals-could be observed. Sophisticated self-propagating malware was constructed to delete or manipulate data, hardware and physical systems have caused major business disruption to companies worldwide with a significant monetary impact. The amount of ransomware attacks has increased significantly. A growing number of attacks have an impact that extends beyond the original target with a wide systemic domino effect.

Economies have high and continuously growing levels of dependency on IT systems, applications and software contributing to the systemic exposure. Growth in connectivity between digital and physical worlds as well as the progress in commercial deployment of Internet of Things and Artificial Intelligence will translate into new vectors of cyberattacks and further increase risk aggregation effects. These changes translate into new challenges for the next phase of cyber defence.

Regulations on data protection and storage locations to provide governments with better control over their data are being implemented worldwide. The rationale for this control is founded by privacy, censorship and anti-terrorism concerns; compliance with new regulations likely results in operational changes for companies.

Albeit, to cope with the global cyber threat it is of rising importance for the institutions in this environment – governments, regulatory authorities, law enforcement agencies, the legal and audit professions, the non-government policy community, the insurance industry and others – to cooperate, this remains ambitious. Cyber risk defence can only be effective if these groups share a common understanding of the changing nature of the threats, their importance and increased interconnected nature. If working individually as well as jointly, these groups have the ability to increase the collective cyber resilience. Therefore, it is vital for all institutions to collaborate and share knowledge.

From the insurance perspective, there is no single standard policy to cover cyber risks as the characteristics of cyber threats vary widely across industries and corporation sizes, whilst the terms and conditions of policies can be complicated at times. Thus, companies need to have a deeper understanding of their own exposure as it will help determine the appropriate type and amount of coverage required based on their risk tolerances. Furthermore, organisations need to be cognisant that a cyber insurance policy is only one of many tools that form a more comprehensive cybersecurity management strategy.

Supporting organisations to identify the right balance between cybersecurity investments and transferring residual risk by means of comprehensive insurance products is a key task of the insurance industry.

Information as of 2020
www.hannover-re.com

hannover re®