the CHARTERED INSTITUTE of LOSS ADJUSTERS

CILA

Cyber – A view from European Risk Managers

By Malcolm Hyde Bsc (Hons) Dip (Fr) FCII FCILA FUEDI-ELAE

December 2019

Introduction

This paper is intended to assist members of the Chartered Institute of Loss Adjusters in understanding the perception of cyber risks as seen by Risk Managers. It is based on information published by the Federation of European Risk Management Associations to their members when they consider cyber risk. In addition it provides an outline of some typical cyber insurance coverages that are available. The full FERMA document may be found at https://www.ferma.eu/advocacy/preparing-for-cyber-insurance/

The World Economic Forum has identified cybersecurity as one of the top five risks faced by governments, organisations and civil societies across the world. This assessment is based on increasing cyber-attacks and massive data frauds. Cyber risks are therefore important to understand.

Risk Managers view insurance as one of a set of tools to build resilience to cyber threats. Insurance solutions offer - prevention advice, mitigation support and monetary pay outs for costs incurred as a result of a cyber related incident. The variety of covers range from tailor-made cyber insurance to “off the shelf covers”.

Risk Factors

Loss Adjusters are charged with verifying that the risk is in fact the same as the risk presented. Understanding the risk factors used by Insurers is therefore important. The following is intended to assist Loss Adjusters in understanding typical but not exhaustive factors used by Insurers.

The following information is typically assessed by Insurers in order to evaluate the extent of an organisation's exposure to cyber threats and to better assess what insurance solution to offer and on what terms. This is an outline and is neither exhaustive nor mandatory.

Risk factors and why some are relevant are as follows:

- Business sector, type of products and services supplied
- Percentage of activity in business to consumer (B to C)

  B to C can involve processing personal-data customer banking details which can create greater risk of third-party loss

- Percentage of B-to B (Business to Business)
- Geographical area (countries, jurisdictions)

  Single or multiple locations of supply chains and differing laws in different jurisdictions are all relevant

- Turnover/Income

  This is considered to be the strongest indicator of potential exposure

- IT Security budget

  This budget expressed as a percentage of overall budget shows a commitment to cybersecurity.

- The extent to which awareness is raised in the business – Training of operational teams as well as the IT team
- Ability to map all physical systems and data within these systems, in particular the ability to map the more sensitive information and servers.
- Methods of authentication to access IT systems
- Mobile working security policies

- Networks

  Networks should be partitioned so that only those who need access are granted access. Insurers will be looking for what data can be accessed and by whom (for example HR and salary information should be separated / partitioned)

- Secure Administration

  This includes the strictness of password protocols, allocation of correct rights to information, prohibition of access to the internet from servers used by system administration

- Industrial Control Systems

  This relates to the extent to which a business relies on the integration of hardware and software with network connectivity in order to support critical infrastructure. The greater the reliance on network connectivity, the greater potential for a large interruption loss in the event of a cyber-attack.

- IT Suppliers

  Adequate and appropriate procurement procedures should be in place

- IT Update Management

  Here Insurers are concerned with the processes in place to ensure hardware and software is updated as it becomes unsupported

- Ongoing Assessment

  Organisations should have robust processes to evaluate whether a cyber-attack has occurred or is on-going

- Personal Data

  Personal data is potentially high risk and sensitive personal data is a greater risk. An organisations retention, use and protection of this data is a considerable risk factor

Key Coverages available

The coverages available can be divided into the following:

1. *Prevention*
    a. Pre breach assessments
    b. Access to pre-vetted vendors
    c. Cybersecurity information
2. *Assistance*
    a. Forensic investigators
    b. Legal services
    c. Notification
    d. Credit monitoring
    e. Relevant call centre services
    f. Crisis management and public relations
3. *Operations*
    a. Costs incurred to keep the business operational or return it to its operational state
    b. Loss of revenue, income, turnover
    c. Costs incurred to recreate/restore data and information
4. *Liability*
    a. Legal costs and damages from claims alleging privacy breach or network security failure

The purpose of this paper was to set out some of the typical risk factors used by insurers to decide whether to accept a risk, on what terms to accept the risk and at what price. In addition it has set out some of the typical covers provided and is therefore a high level overview and is deliberately not a technical commentary on the covers provided nor technical in terms of claims handling.