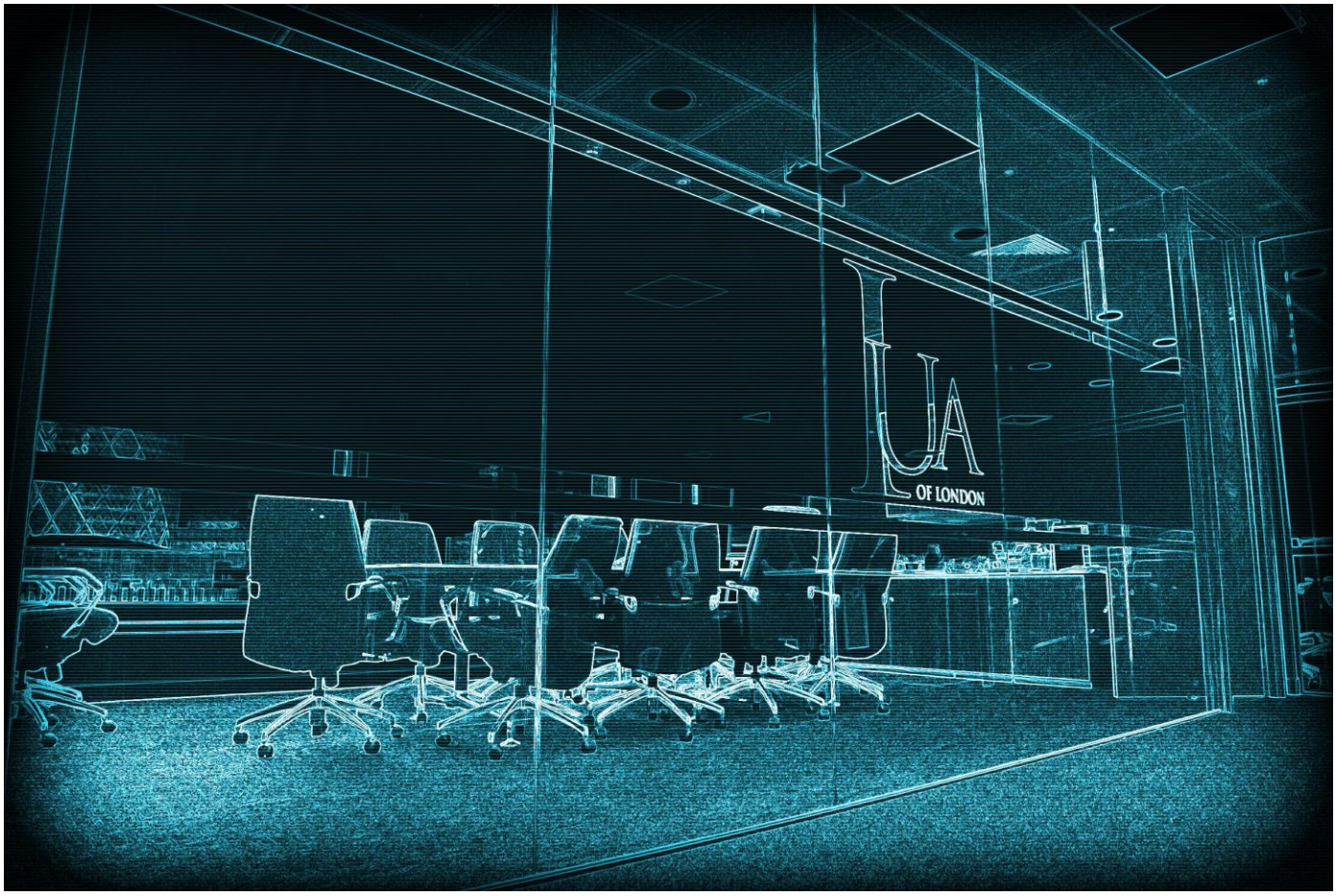
International Underwriting Association



IUA Cyber Underwriting Group

Policy Positions

January 2018

IUA Cyber Underwriting Group Policy Positions

A report from the IUA's Cyber Underwriting Group

With thanks to the IUA Working Party:

Matthew Hogg (Liberty Specialty Markets)
Neil Arklie (Axis Specialty Europe Plc)
Lisa Hansford-Smith (XL Catlin)
Matthew Webb (Hiscox)

This publication is intended to convey the committee's general positions with regard to cyber risk. It is not, and is not intended to be, a complete statement of underwriting practice relating to this area. It should not be relied on or be used as a substitute for legal advice in relation to any particular set of circumstances. Accordingly, the IUA does not accept any liability for any loss which may arise from reliance on this publication or the information it contains.

First published 2018

Table of Contents

Preamble

The note below represents a précis of the key cyber issues currently under discussion by the IUA's Cyber Underwriting Group (CUG). It is not intended to be exhaustive and is subject to change as developments occur. It has been drafted to indicate the Association's broad policy position when in discussions with third parties, focussing specifically on a London market / UK emphasis.

Headline Messages

- ✓ **Traditional classes of business do not usually provide comprehensive cover for cyber incidents. There are often gaps in the cover of the traditional class policies that require extensions or the utilisation of specific cyber products.**
- ✓ **There is a wide and competitive range of cyber insurance products available in the UK and European markets.**
- ✓ **The growth of the cyber threat and the insurance industry response has taken place with such speed that underwriting talent, data acquisition and sophisticated modelling of cyber exposure are highlighted challenges. The same can be said for the reinsurance capacity for cyber.**
- ✓ **The education and increasing awareness of clients in respect of their potential cyber liabilities, the law and commercial security options, particularly on the benefits and limitations of insurance, should be promoted. Stronger action by national authorities is needed to promote this education.**

What is Cyber Insurance?

The word "cyber" has unfortunately and almost irretrievably been linked to insurance policies as nomenclature for a number of various perils. Many of these perils are only vaguely, or sometimes completely unlinked to cyber, which might roughly be defined as "relating to or characteristic of the culture of computers, information technology, and virtual reality". More precisely Cyber Insurance, as a stand-alone product, has instead looked to provide cover for:

i) computer network integrity exposure, and;

ii) privacy, confidentiality and network security liability exposures.

In other words, cyber has looked to cover the risks brought by Information Technology (IT) and technology more widely, but also for both digital and non-digital data. Other exposures have then been further attached to this on occasion.

This broader view of what cyber insurance might look like and include does lead it to naturally extend beyond the current predominance of privacy insurance (mainly driven by the US market), but into areas where the weaknesses of inherent technology within global business products and services will be underwritten.

Policy Positions

Cyber Exposure in Other Classes of Business

There can be elements of cyber cover either explicitly or implicitly contained within other insurance products in the market. A “soft” market is driving cyber coverage into other product lines where there is limited underwriting expertise. Typically, a stand-alone cyber policy is purchased due to the following gaps in standard products (high level assessment only):

Professional Indemnity/E&O

- Cover not provided unless the loss occurs in the ‘ordinary course of your professional services’;
- No cover for claims by employees;
- Unlikely to cover malicious or unauthorized use of Insured’s own network to damage, misuse or destroy its clients’ data or to cause a denial of service attack (unless it is a Tech PI/E&O policy);
- Computer virus transmission is often excluded (unless it is a Tech PI/E&O policy);
- Cover is often restricted to claims made by an Insured’s client and not by Banks, Payment Card Industry etc.;
- Usually no cover for fines and investigations by a regulator;
- Generally, only third party cover is given, so there is no cover provided for customer care and reputational expenses, such as costs of notification, credit monitoring and Public Relations, or for loss of business income, damage to digital assets, cyber extortion or reputational damage.

General Liability

- Only covers bodily injury and physical property damage;
- Data has been deemed by courts to be an intangible form of property;
- Business interruption cover is usually only given if losses arise out of material damage; not if arising out of non-material damage to network;
- Computer virus, damage to data and network exposures are typically excluded.

Computer All Risks

- Only covers costs for repairing damaged hardware (tangible property).

Crime insurance

- Usually limited coverage for money, securities, or “tangible assets”;
- Often must be a “loss” and a “gain” to trigger coverage;
- Identification of the perpetrator(s) is sometimes required;
- Does not address the business income loss or any liabilities;
- May contain a ‘Voluntary Parting Exclusion’ which could exclude many losses due to social engineering/phishing attacks.

Systemic Loss

- *Technology dependencies and socio-economic factors create systemic risk*

Dependencies upon an often limited number of software and hardware services and solutions are arguably the most apparent systemic risks. Consideration should be given to the prevalence of certain cloud computing platforms to small and mid-sized retail companies, or the limited number of Industrial Control System manufacturers in heavy industry and critical infrastructure. Commonality of technology can be found both within and across industry sectors. The internet is a clear example of systemic risk, while others are more subtle.

Technology-based dependencies may not be the only systemic risk. Socio-economic risks exist that may be technology or industry agnostic, such as risk qualities that draw attention from hacktivist, terrorist or state-sponsored groups. Whilst underwriters in non-cyber lines will invariably have limited knowledge of “cyber” exposures generally, the implications of systemic risk have historically been rarely understood or modelled. Attention has now been brought to the aggregational impact of cyber exposures, both within traditional lines and stand-alone cyber, by Lloyd’s and the Prudential Regulation Authority (PRA).

The implications of a more robust approach to aggregation and realistic disaster scenarios include the following:

- Increased Research and Development (R&D) into scenarios and exposures;
- Standardisation of data and policy definitions;
- Cyber modelling;
- Industry v Government accountability and resilience;
- Risk Appetite and Capital Modelling.

Standards in Data Collection

- *Insufficient data about the frequency and cost of cyber claims – more work needs be done where possible.*
- *Need for coherent and consistent recording of cyber incidents.*
- *Assessments and policy making in general would benefit greatly from better data on incidents.*

Within the boundaries of European and UK legislation, the IUA supports information exchange and communication between key stakeholders on cyber issues and claims. Thus, we would welcome the establishment of a cyber incident record / registry system that collected and shared statistical data on the cost and frequency of cyber losses and claims in Member States. However, the IUA's CUG recognises the difficulties in establishing robust claims data and trends, given that claims notifications are often put on hold as long-term investigations take place. Furthermore, we recognise that the interpretation of data collection may be complicated by the use of differing collation methodologies and terminology across Member States.

Ultimately, insurance companies do not hold all of the answers. The role of Government, regulators and other vendors will be critical to establish any useful data for underwriting purposes, as well as for any extrapolation for risk management and advisory purposes.

The IUA is supportive of initiatives aiming to increase the efficiency of collecting claims and underwriting data in order to bring greater transparency and maturity to the market, . For example, the IUA is particularly supportive of the Lloyd's "Common Core" data standards that intend to assist in building a common language amongst carriers and regulators with regards to cyber and so as to specifically improve market capabilities with regards to the modelling of systemic risk and more accurate and professional underwriting. The IUA remains an interested party in all matters relating to data collection standards and will seek to be both fully informed and engaged in any further developments.

Promoting Awareness, Education and Advice

- *IUA strongly supports the cooperation of industry associations, financial security associations and competent authorities in promoting cyber risk awareness amongst operators.*

It is essential that national competent authorities, insurers and brokers continue to educate companies at operational risk management level and in the boardroom about their cyber risk exposures. Information on the status of the UK (and, where applicable, other) cyber insurance markets with explanations of the coverage options available to them is important to ensure that they can obtain the most suitable security for their risk.

As part of a wider education process, one needs to consider and analyse further the pros and cons of existing cyber risk products and extensions to more traditional classes of business – identifying possible problem areas, gaps in coverage and uncertainties.

Furthermore, continuous professional development of insurance practitioners in the cyber market is essential to further a respected and educated marketplace which has rigour in its approach in providing meaningful cover to the satisfaction of all stakeholders, including regulators.

The consideration of R&D projects, some through collaboration with third parties, will be a necessary requirement of the IUA's CUG on matters of insurance and cyber exposure.

The IUA's CUG will also focus on legal and regulatory matters relating to insurance law, as well as data and privacy matters through a Sub-Committee populated by experienced legal and claims professionals.

Representing Good Underwriting Practice

In representing good underwriting practice for Cyber, the IUA's CUG must represent sound underwriting practice generally for insurance and specifically for cyber. More generally it will focus on:

- Meaningful collection of the material facts required for underwriting, in addition to information pertinent to underwriting cyber exposures;
- Sound analysis of the collected information;
- Sound classification of a risk in its exposure environment;
- Sustainable selection and rating of risks including management of exposures;
- Managing a portfolio of risks to the satisfaction of all stakeholders;
- Adherence to all insurance laws, ethics and regulations pertinent to underwriting;

Whilst there are degrees of complexity to good underwriting practice within Cyber, at a high level across a portfolio there are specific trends that must always be monitored, some examples are provided as follows:

- Governmental, legal and regulatory environment
- Systemic risks and aggregation
- Technological development
- The socio-economic risk and the threat environment

When a company of any size is looking for cyber insurance, it is critical that sufficient information is provided to brokers and underwriters in order to develop a detailed picture of the risk. For many companies this may be the first time that they have had to provide cyber related information as part of an insurance submission. Many companies find it difficult to determine what information they should provide and, in many cases, where this information be obtained.

One of the main questions asked is what type of information should be provided by an insured and, therefore, what a good submission should look like. While there is no one size fits all approach, there are common areas of exposure detail that cyber underwriters are looking for which can be categorised for companies of all sizes into four broad categories:

1. **General Risk Management Overview**
2. **Information Technology and Security Risk Management**
3. **Data Risk Management**
4. **Business Continuity and Disaster Recovery Planning.**

These areas link closely together and can be useful in assisting an insured in presenting information to insurance carriers as it enables the underwriters to rate the cyber risk. Whether such information is provided in an application form, or as part of a submission, is not as relevant as providing a clear overview of the company and their processes/procedures. There is the potential for an underwriter to take a more negative view of a risk when buyers provide little or no information as requested. This is a complex and important area of coverage, providing for both first and third party exposures and buyers, brokers and underwriters need to work together to ensure that the risk is protected as comprehensively as possible.

The IUA's CUG will stand to represent all of the above, as well as matters of a more technical nature relevant to insurance or cyber risk.

The area of risk management is expanded upon on Page 11 of this document.

Government Interaction

In 2010, the UK Government rated cyber-attacks as a Tier 1 threat which led to the Cabinet Office publishing the UK Cyber Security Strategy in 2011, setting aside £650 million to develop a response for the UK. The Government updated the National Cyber Security Strategy in 2016 and pledged to invest a total of £1.9 billion over the next five years to transform the UK's cyber security. The vision for 2021 set out in the strategy aims to ensure that the UK is secure and resilient to cyber threats, while remaining prosperous and confident in the digital world. Three objectives were outlined as follows:

- **Defend** – The UK has the means to defend the UK against evolving cyber threats, to respond effectively to incidents, to ensure UK networks, data and systems are protected and resilient. Citizens, businesses and the public sector have the knowledge and ability to defend themselves.
- **Deter** - The UK will be a hard target for all forms of aggression in cyberspace. The UK has the ability to detect, understand, investigate and disrupt hostile action taken against it, pursuing and prosecuting offenders. The UK has the means to take offensive action in cyberspace, should it chooses to do so.
- **Develop** – The UK has an innovative, growing cyber security industry, underpinned by world-leading scientific research and development. It has a self-sustaining pipeline of talent providing the skills to meet the national needs across the public and private sectors. The UK's cutting-edge analysis and expertise will enable it to meet and overcome future threats and challenges.

As a result of the Government's strategy we have seen many initiatives set up such as the National Cyber Crime Unit, Cyber Essentials, Cyber-security Information Sharing Partnership and, in 2016, the establishment of a single, central body for cyber security - the National Cyber Security Centre.

This in turn led to Government collaboration with the UK's insurance market, beginning in March 2015. The purpose of this collaboration was to help firms get to grips with cyber risk; to establish cyber insurance as part of firms' cyber toolkits and to make the UK a world centre for cyber security insurance. As part of the project's recommendations, the Government committed to work with the insurance industry to establish a forum for data and insight exchange and for policy discussions. One of the main goals of the forum is to work to improve the information available for underwriting and determining aggregation risk. The IUA has an 'open arms' policy with respect to Government interaction and is represented on the Cyber Insurance Forum that was formed by the Cabinet Office in 2015. The forum is now under the remit of the Department for Digital, Culture, Media and Sports.

On an ad hoc basis it is anticipated that the Secretary, Chairman or Deputy Chairman of the IUA's CUG Committee will be asked to advise, support or simply engage with government entities on the basis of co-operation with the IUA. At all times, any representative of the CUG shall endeavour only to share the views of the CUG, unless expressly caveated that any views stated are made in a personal capacity or with regards to their company market employer.

Model Wordings / Clauses

The IUA's CUG recognises that cyber is an evolving landscape where wordings, exclusions and clauses will continue to respond to new regulations, technologies and exposures. We will look to identify trends that need to be addressed by the cyber insurance market and other lines of business.

In many property, marine and casualty lines standardised exclusions have been applied, for example:

- Institute Cyber Attack Exclusion Clause CL380;
- Terrorism Form T3 LMA3030 Cyber Exclusion;
- Electronic Data Exclusion NMA2914 Extract.

The IUA's CUG will look to advise on and develop standard clauses, where it makes sense to provide guidance to the market. There has been a general immaturity in market wordings and clauses for cyber insurance, given the development and speed of the insurance class and the rapid change in exposures.

Regulation – UK and EU

Law makers in the UK, across the EU and globally are introducing new legislation in relation to cyber. The purpose of which is to modernise the legal frameworks within which organisations operate, considering the increasing reliance on the digital environment at both individual lifestyle and global economic level. Clearly, this has a direct impact on the insurance solutions that are offered. The IUA will offer opinion or commentary on any relevant legislation if applicable to the group and will lobby relevant bodies on the basis of positions agreed by the committee.

Media Policy

With respect to the committee's position in the media, members of the committee will not purport to express the opinion of the committee, unless the position has been discussed and agreed by the committee beforehand. Members may comment in the media as a member of the committee, but will not do so as a spokesperson for the IUA. Any issues of significance or situations that are of a particularly controversial or sensitive nature, should be referred to the IUA before any comment is made in order for an agreed approach to be developed and approved by the committee.

It is the responsibility of individual members to ensure that in respect of any public event or engagement with the Media, the position is made clear as to whether a Member speaks on behalf of the IUA, their company employer or in any personal capacity.

Risk Management

The IUA's CUG recognises that risk management for cyber exposures needs to adapt to evolving threats and be versatile to achieve resilience. The appropriate risk management would also vary by industry and size of the organisation. The aim is to achieve security of its critical assets, including protected data and intellectual property.

The above diagram represents a generalised risk management process. The implementation of this process to individual risks may be necessary for the cyber market. Cyber has unique aspects that should also be considered carefully, including but not limited to:

- Organizational, technical and governance safeguards.
  These would look at how a firm would assess and respond in a timely manner to a cyber incident.
- Sensitive Information safeguards.
  Organisations have a varying level of liability for the information they hold and would need to understand these responsibilities and how to handle any breach of these liabilities.
- Access controls.
  A large proportion of cyber incidents are caused by internal factors, such as employee theft or losses caused by external vendors with access to the organisations network. Hence, access to systems needs to be controlled and monitored by the organisation or an external assessment should be in place.
- Business Interruption and continuity safeguards.
  The organisation would need to have a business continuity plan that includes a disaster recovery plan in place that makes provision for a cyber incident.
- Physical safeguards.
  Cyber incidents can occur to physical assets and the organisation should assess the protections in place.
- Security and data awareness training.
- The socio-economic threat, including the role of "bad actors", and their motivations

A risk assessment by its own risk engineer, independent firm or in the form of a questionnaire would be desirable. This will allow an underwriter to be able to assess the security maturity within a company.

General Risk Management Overview

An understanding of how the General Risk Management of the organisation operates (centralised, decentralised etc.) as the latter categories will feed into the general risk management philosophy of the insured.

Information Technology and Security Risk Management

An understanding of how a firm's Information Technology and associated securities are managed, how reporting to senior levels take place and the thought process behind the defence of the network are key areas that underwriters consider when assessing a risk. Questions around the technology vendor supply chain and how vendors are reviewed/assessed are also important parts of the underwriting process.

Data Risk Management

The data a firm holds and how it is protected is another key area from an underwriting perspective. The types of data (credit card, PII information, sensitive personal data, intellectual property etc.) held on the system, along with how it is protected/encrypted and whether there is any payment processing that is being carried out is information that is relevant to the rating of a risk.

Business Continuity and Disaster Recovery Planning

It is critical to gain an understanding of how a business will operate if there is a system failure/system downtime. How long the business can operate without the IT System, what the incidence response plan is in order for operations to continue and how the system will be re-established are factors that give a better overview of the preparedness of the business.

ENDS

International Underwriting Association

1 Minster Court
Mincing Lane
London
EC3R 7AA

Tel 020 7617 4444
Email info@iua.co.uk
Web www.iua.co.uk
Twitter @IUAofLondon

The International Underwriting Association of London (IUA) is the focal representative and market organisation for non-Lloyd's international and wholesale insurance and reinsurance companies operating in the London Market. It exists to promote and enhance the business environment for international insurance and reinsurance companies operating in or through London.