CHUBB®

Managing Tomorrow's Cyber Risks And Multinational Insurance

Authored by;

Suresh Krishnan
Head of Major Accounts Division
Chubb Europe

Jared Concannon
Major Accounts Segment Leader,
Cyber - Europe, Eurasia & Africa, Chubb

Helen Bourne
Partner, Clyde & Co LLP

Rosehana Amin,
Senior Associate, Clyde & Co LLP

CLYDE&CO

Introduction

Our latest multinational report, written in conjunction with Clyde & Co LLP, analyses the current international cyber risk landscape and highlights areas that a multinational corporation should consider to prevent, protect and manage data privacy and cyber incidents.

Cyber risks and insurance solutions are evolving continuously. In this report we review the key cyber risks as we see them today and how we envisage them in the near future. We identify the largest and most recent examples of first party and third party losses affecting multinational corporations, and we analyse the cross-border challenges within key global jurisdictions where stricter regulatory regimes have focused on protection of data privacy.

Finally we consider how major multinationals need to engage with experts from both within their own business and externally when mitigating and managing cyber risks. Starting with the risk management teams and including IT and technology experts, multinationals must also incorporate those responsible for compliance and regulation in addition to their insurance broker and multinational insurer. A team of multi-disciplined experts with a clear multinational plan are necessary when building a cross-border cyber prevention, protection and mitigation programme insuring global exposures.

All content correct as of May 2019)

What are the evolving cyber risks?

Cyber risk continues to evolve with no profile limitations such as national borders, types of data or industry classes. Several factors contribute to a multinational company's cyber risk profile and proactive steps need to be taken to address these risk exposures. They include:

Evolving threat landscape: Threats are diverse and ever-changing while vulnerabilities morph as global organisations become increasingly reliant on technology to assist with electronic processes [for example the Internet of Things (IoT) and computer networks] and operation of critical infrastructure. As data continues to become an increasingly valuable commodity, these new vulnerabilities will be exploited through cyber attacks.

Global nature of data breach incidents:

- In 2018, a large company within the hospitality sector experienced unauthorised access to its database compromising up to several hundred million customers' personal records on a global scale.
- In 2019, sensitive information known as "Collection #1" was published on the internet allowing anyone to download a collection of hundreds of millions of email addresses and passwords. The cache of data has been built up from numerous data breaches, across various countries, over a decade.

Supply chain risks: Many companies operate a complex global supply chain that is vital to the successful development and delivery of the final product to the end customer. These supply chain structures now face new risk of disruption from potential cyber attacks. This threat requires companies to regularly analyse how exposed their supply chain is and how a disruption may impact their business operations.

Third party risks: There are also risks to businesses created by third party vendors that are increasingly connected to the primary business, and whose systems may not be as secure or robust. This connectivity broadens the cybersecurity threat landscape because vendors, such as building maintenance companies, may now, inadvertently, have a higher level of system access.

Risk management: In addition to the evolving external challenges companies face, risk managers are also challenged with defining where cyber risks fall within their organisation's insurance profile, and evaluating just how their insurance programmes protect them in the event of first party or third party cyber losses. Additionally, unlike comprehensive standalone cyber insurance policies, potential silent cyber cover (i.e. non-affirmative cover) in traditional insurance lines does not expressly address or consider the extent to which a cyber risk will be covered, which creates uncertainty for companies. Businesses also need to ensure they are continually reviewing their cyber security policies and procedures, ensuring compliance with data privacy laws (including those with extra-territorial reach) and implementing proactive risk mitigation strategies within their organisation (e.g. penetration testing, security training and technical controls) to stay ahead of a fast-moving cyber landscape.

What and where are tomorrow's losses?

First party exposures

Typically as a first line of defence following a cyber incident, companies are faced with various first party expenses as they work to contain and mitigate the damage from an event. These costs may include:

- Engaging third party IT firms to assist in investigating, identifying and defining the scope and severity of the incident
- Utilising external legal resource to ensure compliance with the range of regulatory requirements including a risk assessment analysis, considering implications of a data breach, notification obligations to impacted individuals and reporting to regulators
- Assistance in providing notification to impacted individuals and perhaps with credit and ID monitoring services for those individuals as well
- Public relations costs as the organisation works to manage the external messaging and communication of the event to minimise the reputational damage to the company.

If the cyber event impacts the availability of IT resources, the company may face a reduction in business income during the down time, as well as additional costs to get the business back to full operating condition including increased costs of labour.

Third party exposures:

Claims by third party data subjects in relation to the misuse, disclosure, or destruction of confidential information stored in a company's network. These can include privacy claims, contract and tort claims and could also include other statutory actions (e.g. actions under copyright, defamation laws). Privacy claims may include (depending on the jurisdiction) claims for non-material (i.e. distress) damage.

Companies and their D&Os can be exposed to claims from data subjects or shareholders subjecting them and the enterprise to litigation. This could result from a cyber event that adversely impacts the share price or an event concerning the release of data. Companies could be held liable for:

- failure to implement (and constantly review) effective systems and controls to prevent breaches
- the financial impact on the business due to a large fine or reputational damage
- failure to respond effectively to a breach
- failure to notify in time under the mandatory notification requirements in the General Data Protection Regulation (GDPR).
- vicarious liability for rogue employees who expose data
- criminal liability depending on the jurisdiction: For example in the UK, breach of the two new criminal offences in the Data Protection Act 2018 (intentionally or recklessly re-identifying individuals from anonymised data; and altering records with the intention of preventing disclosure of that information following a subject access request).

International legal and regulatory exposures: A comparative overview

Data protection regulation has become more complex and holds global companies to account over the processing, control and aggregation of data across national boundaries (e.g. the GDPR). Sector regulation is becoming more targeted on cyber risks e.g. financial services regulation and national critical infrastructure regulations.

A multinational company's cyber preparedness extends beyond ensuring its IT systems are secure and robust or guarding against the vulnerabilities of third party vendors or supply chain risks. A global company must also be aware of the relevant legislative requirements for data protection in the countries they operate and understand their main obligations.

Risk managers and data protection officers of global companies need to ensure that policies are in place, data protection impact assessments are carried out and training is provided to staff so that the legal requirements are properly understood. In some instances, data protection laws have extra-territorial reach. Accordingly, while a company may not operate in a specific country, it may still be subject to the requirements in force in that country, so the assessment of the regulators needs to extend beyond the immediate jurisdiction.

While not intended to be comprehensive, we canvas below the patchwork of data protection laws of which multinational companies should be mindful:

European Union:

The GDPR is the key EU law governing data protection which came into force on 25 May 2018. It applies to all businesses and organisations, including those located in other countries where they offer goods and services in the EU. The GDPR imposes a requirement to report any personal data breach without undue delay and within 72 hours and failure to comply or a breach in the regulations generally may result in substantial fines.

Americas

- **The US** has a patchwork of national privacy laws and regulations, however, several states are expected to pass significant privacy laws. In California, for example, the California Consumer Privacy Act of 2018 will be effective from 1 January 2020.
- **Canada** has a comprehensive regime for the collection, use and disclosure of personal information.
- **Latin America:** In Brazil for example the LGPD is the country's first comprehensive data protection regulation and it is largely aligned to the GDPR. It will go into full force in August 2020.

Middle East & Africa

- **South Africa:** The Protection of Personal Information Act 4 of 2013 has been enacted, but only certain provisions are in effect currently, with the remaining provisions expected to take effect in 2019.

Asia Pacific

- **Australia:** The Commonwealth Government committed to implement a Consumer Data Right (CDR) which allows a consumer to obtain certain data held about that consumer by a third party and require data to be given to accredited third parties for certain purposes. The current intention is that the big four banks will participate in a pilot of the CDR from 1 July 2019 to 31 January 2020.
- **China:** There is no single comprehensive data protection law. On 1 June 2017, the PRC Cybersecurity Law came into effect and became the first national-level law to address cyber security and data privacy protection.
- **Hong Kong:** There are no restrictions on transfers of personal data to third countries. There is talk of the implementation/enforcement of s33 of the Personal Data (Privacy) Ordinance regarding the transfer of data outside the jurisdiction.
- **Singapore:** The Personal Data Protection Act regulates both the collection and use of personal data but does not apply to the public sector, to whom separate rules apply. It is anticipated that the Act will be amended some time in 2019 to incorporate the changes proposed in the PDPA Consultation which concluded in 2017 focusing on "approaches to managing personal data in the digital economy," with topics including "challenges for alternatives to consent" and mandatory breach notification.

Looking to the future

As more personal data is being processed, internationally, there is more risk for a company to ensure that it protects cross-border transfer of information especially where a country's data protection laws require that the outbound transfer of such data receives a standard of protection comparable to the protection under the originating country

However, companies need to bear in mind that international frameworks with reciprocal recognition of data protection regimes do bring benefits to citizens and businesses as they facilitate commercial exchanges. Examples include;

EU-US Privacy Shield

This protects the fundamental rights of citizens whose personal data is transferred from the EU to the US and brings legal clarity for similar data transfers.

EU-Japan Adequacy Decision

In January 2019, the EU adopted its adequacy decision on Japan, creating the world's largest area of safe data flows allowing personal data to flow freely between the two economies.

International transfers with the EU

Other third countries which provide adequate levels of protection allowing for safe transfer of data outside the EEA include: Andorra, Argentina, Canada (only commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the USA. There are also adequacy talks ongoing with South Korea.

Complementing indemnification with local tailor-made services including local claims handling and payment, incident response in the local language with local capabilities and expertise.

Technology and commercial realities often outpace rules and regulation, but how does multinational cyber liability insurance play a role?
Although cyber and technology risks present unique, rapidly evolving challenges to risk management within a global organisation, it is imperative to maintain engagement with key stakeholders throughout a business to map out future cyber related exposures the organisation may face. The difficulty in keeping pace with changes in the technologies a business uses, and the various global regulations that govern them, highlights the value from consulting with a broad spectrum of internal and external experts who can counsel and direct how to structure a robust and flexible risk transfer multinational cyber insurance programme.

Reviewing claims data helps provide a better understanding of how the risks themselves are evolving:
Engaging with multinational insurers and brokers can provide unique insights into the types of events causing cyber claims globally. For example, although types of ransomware have evolved significantly over time, paralysing a business through a ransomware attack continues to drive cyber claims experience across the globe. Ransomware, historically, were targeted extortion schemes aimed at quick pay-outs for cyber criminals. The types of ransomware that clients face today can be either indiscriminate or targeted and seek significantly higher payment demands. Ryuk, is a recent example of a ransomware variant that is often coupled with a banking trojan, allowing the extortionist access to a company's financial data providing them leverage in ransom negotiations. As the ransomware threat evolves, companies are faced with complex, time sensitive decisions to resolve these extortion threats.

Building a fully integrated multinational cyber insurance programme promotes responsible corporate governance
As cyber risks evolve and do not discriminate among national borders, the value of local cyber policies with commensurate claims and response services cannot be underestimated.

Local policies tailored to local regulations and terms and conditions consistent with locally acceptable customs and practices are prudent for effective local coverage. Supplementing local requirements with international standards brings robust protection for local subsidiaries, affiliates and joint ventures while protecting the reputation of the entire enterprise.

A broad global umbrella master policy providing drop-down coverage to fill gaps for differences in conditions and local limits brings efficiency in pricing and needed capacity.

An effective cyber multinational insurance programme combines appropriate indemnification with responsive service. What questions should be asked when building a cyber multinational insurance programme?
As cyber risk continues to evolve and permeate new parts of businesses that previously did not face cyber exposure, it is imperative that clients not only have bespoke risk transfer insurance coverage but also are supported in identifying emerging risks and in responding globally to cyber events. The following checklist is useful guidance for the risk professional managing cyber exposure when building a sustainable multinational insurance programme for a global organisation.

Cyber Multinational Liability Check List

- Have I mapped out how my multinational cyber insurance programme fits into and complements my organisation's global and local cyber incident response plans?
- Where do I want my cyber insurance claims to be paid? Does my multinational cyber insurance programme have local policies placed in countries to facilitate the payment of claims to local offices?
- Does my multinational cyber insurance programme allow for the flexibility to react and respond differently to cyber incidents and cyber claims in countries depending upon my company's local capabilities?
- Does my multinational cyber insurance programme provide coverage for data and privacy regulatory fines and penalties where insurable by law? Does my multinational programme contain any restrictions to that limit offered?
- Does my multinational cyber insurance programme offer emergency local country and local language expertise in cyber incident response services (forensics, PR, etc.)? Can those expenses be insured reimbursements to my company in the impacted country?

Conclusion

Staying ahead of the evolution curve in cyber liability will be challenging

From a risk management perspective, it is vital for global organisations to have access to a multidisciplinary team of experts, to analyse the evolving threat landscape and regulatory regimes affecting the specific industry class in which the company operates, and to review peer and non-peer affected claims and incidence review points. These are all good starting points to build a multinational cyber insurance programme.

As criminals demonstrate their innovative abilities, and increase the potency of attacks, a multinational organisation is challenged to keep pace with the change in threats faced. It is crucial to note that cyber liability insurance policy forms will evolve as customers demand specific coverages based on incurred and anticipated losses. In addition, the scope, breadth and limitations in cyber policies can be supplemented by emergency cross-border incident response services to mitigate and manage potentially non-indemnifiable losses.

Understanding the evolving national scrutiny of a multinational enterprise's data privacy standards will be a key factor to staying ahead of the evolution curve. In addition to the threats cyber criminals pose, many nations are working to govern data and technology to better protect consumers. While there are various privacy and data regulatory regimes in force, or soon to be in force, it is unmistakable that the momentum is moving in one direction - increased regulation and scrutiny into the way companies handle and manage data.

Finally, it is important to pull this all together. Collaborate with an insurer and broker with international subject matter expertise, product knowledge and servicing capabilities as well as with internal and external IT and compliance expertise. This combination enables parties to collaborate, plan and document a clear risk-transfer or risk-financing cyber strategy complemented by an appropriate transfer of excess risk, and ensure the multinational programme achieves performance certainty.

For more information visit our website:
Chubb.com

Chubb. Insured.℠