1. See Home Indemnity Co. v. Hyplains Beef, 893 F. Supp. 987 (D. Kan. 1995), aff'd, 89 F.3d 850 (10th Cir. 1996).
2. See In Retail Ventures, Inc., et al. v. Nat'l Union Fire Ins. Co., 691 F.3d 821 (6th Cir. 2012).
3. The Insurance Services Office ('ISO') offers cyber endorsements to its business owners program forms.

John Black Executive Principal
jblack@skarzynski.com

Michael Silvestro Principal
msilvestro@skarzynski.com

Skarzynski Black LLC, Chicago

Emerging trends as cyber insurance comes of age

Compared to other insurance lines, cyber insurance is still in its infancy. This is hardly surprising as even smartphones - which now seem ubiquitous - debuted only ten years ago. The risks from proliferating technology are not well understood, and the legal protections to address these risks are still evolving. John Black and Michael Silvestro of Skarzynski Black LLC discuss the various ways that insurance now addresses cyber related legal and business risks and may continue to develop.

A maturing cyber insurance market

A significant challenge facing cyber insurers is that, unlike in traditional insurance lines, there is not a robust volume of claims for developing actuarial data. Most available claims data is proprietary, and public statistics are difficult to evaluate as many cyber events do not trigger claims and purchasers of cyber insurance have typically been larger businesses in specific industries, such as healthcare or finance. In addition, cyber insurance policies are not standardised, and few coverage disputes have resulted in judicial decisions.

The available claims history indicates that the most compensable losses have arisen under first party coverages, such as breach investigation and notification. While many cyber insurance products insure against third party liability, such as from disclosure of non public personal information, courts generally have not allowed data breach litigation to survive dismissal absent concrete harm, and the principal exposure in such litigation has been defence fees.

Accordingly, evaluating cyber risks involves a higher degree of uncertainty compared to more established insurance lines. In the absence of reliable actuarial data, brokers and underwriters have focused on the insured's relative cyber security - i.e., whether it presents a 'hard' or 'soft' target for potential cyber events. Factors typically reviewed in evaluating a cyber risk include: (1) the volume and type of confidential information, whether personally identifiable information, third party confidential corporate information or sensitive first party information, including intellectual property; (2) the scope and architecture of computer systems; (3) how data is secured, including encryption, multi-factor authentication, and software maintenance; (4) the potential for data to be published or uploaded; and (5) whether the insured must share data between subsidiaries or with franchisees, potentially multiplying exposure points for data exfiltration.

Internal governance over data security has long been important in evaluating cyber risks, including appropriate policies and procedures. Since the Target breach, the security of third party vendors with access to the insured's systems or data has become a greater focus of scrutiny. The fluidity of data, which may flow through networks and systems not within the insured's exclusive control, requires vetting vendors and considering if they should be listed as additional insureds. As companies often rely on multiple hardware, software, and infrastructure vendors, some cyber insurers may ask insureds about contractual data security and indemnification provisions. Downstream and supply chain risks also present challenges. Cyber incidents indirectly affecting suppliers, shipping, manufacturing, or logistical vendors potentially may interrupt an insured's business or result in other potentially compensable losses of business income.

Insurers also consider the potential aggregation of risk from a single event. Devastating events such as the 9/11 attacks illustrate that a single event may cause significant losses across many lines of insurance. If a cyber event were to affect essential internet infrastructure, the losses may ripple out to businesses worldwide.

As the cyber insurance market matures, insurers, brokers and insureds will increasingly look to innovative modeling approaches to evaluate cyber risks. New technologies are already in use, with some insurers partnering with InsurTech companies offering proprietary data sets and predictive models to address underwriting uncertainties. Some InsurTech firms already offer specialised products focusing on cyber risks unique to specific industries, such as automotive manufacturers. Additionally, internet security firms are leveraging proprietary real time monitoring and historical data to develop models to assist in evaluating risks.

Cyber risks and traditional insurance coverages

The growth of connected devices

Image: Marco_Piunti / iStock / Getty Images Plus / Getty Images

Evaluating cyber risks involves a higher degree of uncertainty compared to more established insurance lines.

forming the Internet of Things ('IoT') should accelerate innovation in the cyber insurance market. Billions of additional connected units are predicted to come online in a variety of settings, whether in the living room, on roadways, or in manufacturing. As IoT devices become ubiquitous, their functionality and interaction with the physical world will grow, increasing the potential for cyber events to trigger traditional exposures, such as property damage and personal injury.

Current cyber insurance policies usually provide a mix of third party and first party coverages, albeit focused primarily on the digital world. The forms typically include third party coverages for claims by regulators and third parties for failing to prevent a data breach, harm from transmitting malicious code or content, and media and publication liabilities. Common first party coverages apply to the cost of data breach investigation and remediation, breach notification and credit monitoring, cyber ransom, data asset restoration, reputational harm, and business interruption.

The potential for cyber incidents to cause physical harm through connected devices will require insurers and insureds to evaluate carefully the interplay between cyber insurance and policies in other insurance lines, such as professional liability, casualty, first party property, product liability, crime, and kidnap and ransom. As the volume and types of cyber related claims grow, these complex issues will highlight the need for multidisciplinary approaches to underwriting, broking, risk management, claims handling and coverage analysis.

Casualty

Suppose that disclosure of sensitive information results in allegations of emotional harm; or that industrial equipment is affected by malware, injuring employees; or that a self driving car is hacked, resulting in bodily injury or death. How will existing casualty insurance programs respond?

Demand for cyber casualty coverages will increase as the risk of such events rises and as coverage gaps are identified. Many current commercial general liability forms exclude bodily injury or property damage claims arising from access to or disclosure of personal or confidential information or from lost, corrupted, damaged or inaccessible electronic data. Additionally, some current casualty forms already afford or exclude coverages for on-premises bodily injuries from cyber incidents. How such cyber casualty risks will commonly be insured - through cyber policies, difference in conditions coverages, expansion of traditional casualty coverages, or specialty products - will be an open question for some time.

First party property

Cyber insurance forms that contain first party property coverages are typically limited, including only losses to property directly affected by a cyber incident, such as computer equipment. But what happens when a cyber event causes physical damage to other property owned by the insured? Fortunately, significant losses from this exposure are rare, but they likely will occur with increasing frequency.

Some property policies clearly do not insure this type of risk. For example, named peril policies, commonly issued to smaller insureds, usually do not cover cyber incidents. However, some all risk policies do afford coverage for physical loss or damage resulting from cyber events, although the scope and limits of such coverage varies. Some insurers have developed new policy forms offering cyber coverage for property damage on a standalone or difference-in-conditions basis, with specialty products for specific industries, including the energy sector.

Business interruption

The risk posed by business interruption and contingent business interruption losses from cyber events is also a serious concern. Business interruption ('BI') insurance typically provides coverage for income sustained due to a 'necessary suspension of operations' during a period

of restoration. In the cyber insurance context, this coverage would respond to income losses that could arise from failure of an insured's own systems due to a cyber event. As with traditional BI coverages, cyber BI coverage is typically subject to a waiting period, ranging from hours to days, before coverage attaches.

What constitutes a 'suspension' of operations in the cyber context has not been tested in court, although some courts have held that reduced operations caused by computer troubles do not constitute a 'suspension' of operations triggering BI coverage under traditional first party policies[1]. Given this uncertainty, there is likely to be increased demand for cyber business income insurance, which often differs from traditional BI insurance by not requiring a suspension of business operations and permitting coverage for lost profits from slowdowns or inefficiencies while the business remains operational.

Traditional BI insurance, however, does not apply to losses from the failure of third party vendors or systems, such as a cloud service or supply chain provider. As such, the market for contingent BI insurance for cyber events is growing. Contingent BI risks from cyber events are challenging to assess because they involve the cyber risks of third parties and how they may impact an insured.

Contingent BI risks also present the potential for large losses rippling out of a single catastrophic event, such as the failure of a major piece of software or technological infrastructure. Insurers are mindful of the potential for risk aggregation in a single 'black swan' event, and as such, are approaching cyber contingent BI risks with caution.

Products liability

Suppose an implanted pacemaker is hacked, resulting in bodily injury or death, or that a voice controlled speaker's voice assistant is affected by malicious code and turns on connected home appliances, causing a fire. Many standard products and completed operation coverage forms include broad electronic data exclusions, which could bar coverage for such events. However, some specialty forms affording broader coverages tailored to software developers and connected device manufacturers have already been introduced. Cyber products coverages present the potential aggregation of risk in specific products with higher potentials for bodily harm or property damage, such as vehicles and medical devices, which may limit the availability of this type of coverage.

Crime

Computer crime policies have been available since the 1980s. Although such policies typically cover financial losses caused by computer system fraud, payments or transfers from fraudulent computer instructions, loss of data and electronic media, computer viruses, and forged communications, most forms were developed before the widespread use of the internet. In recent years, courts have extended coverage under computer crime policies for exposures which crime insurers maintain were never intended, such as hacking losses[2]. In response, crime insurers have tightened policy language, sometimes offering limited coverage by endorsement for risks such as email impersonation. At the same time, some cyber insurers offer coverage for first party financial losses caused by computer fraud, payments or transfers from fraudulent computer instructions and social engineering. Whether the crime insurance market will amend policies to offer broader coverage for losses caused through the internet and email systems or cyber insurers will offer more coverage for cyber crime and fraud losses emanating from outside of the insured organisation remains to be seen.

Errors and omissions

The 'Panama Papers' data breach last year, in which over 11 million documents were leaked revealing attorney-client information for more than 214,000 offshore companies associated with a Panamanian law firm, illustrates a significant cyber risk facing lawyers and other professionals. In recognition of this and less widely known breaches at other firms, traditional professional liability insurance markets have responded by offering endorsements to liability policies to enhance coverage for the first party cost of addressing such breaches faced by professionals. In addition, a number of cyber insurers are offering first party and third party cyber policies tailored to lawyers, accountants and other professionals.

Kidnap and ransom

Cyber incidents also pose challenges in managing risks typically insured through traditional kidnap and ransom policies. Some kidnap and ransom policies will respond to cyber extortion attempts, however, existing wordings may require a ransom demand to trigger coverage, which may not always be present in cyber events. Further, what happens when technology is used to facilitate a kidnapping, or to confine or detain individuals? Recently, a Swiss hotel was the victim of a cyber extortion attack that locked the hotel's rooms, confining guests until a ransom was paid. Traditional kidnap and ransom policies commonly include coverage for wrongful or unlawful detention by an agent of, or with the approval of, a governmental entity or insurgent group, but there may prove to be a market for expanded cyber coverage where the offending actor is unknown. Additionally, non traditional purchasers of ransom and extortion insurance may drive demand for standalone or endorsed cyber coverages.

Emerging trends

As technological innovation advances and cyber insurance markets mature, demand from non traditional cyber insurance purchasers will spark growth and fuel innovation in the cyber insurance markets.

Small and mid-sized businesses

Increased demand for cyber insurance products is likely to come from smaller and mid-sized businesses as they recognise their potential cyber risks, including those arising from their possession of customers' personally identifiable information, such as credit card data. Even small enterprises may have thousands of sensitive records, and the potential for significant notification and remediation costs in the event of a breach may present an extinction level event. Small to mid-sized businesses are also more likely to be softer targets for hackers, ransomware and cyber extortionists than larger, more sophisticated entities.

As smaller businesses increasingly seek cyber insurance, markets will respond to meet the demand. Some insurers already offer cyber insurance products designed for small to mid-

sized businesses, with a variety of coverages and limits. Cyber insurance may be offered as a standard component of traditional property and casualty package policies[3], and some property and commercial general liability insurers already offer limited first party and third party cyber insurance by endorsement.

Alternative cyber risk transfers

At the other end of the spectrum, larger and more sophisticated entities will seek alternative cyber risk transfer vehicles. Some large corporations have already begun integrating cyber risk exposures into insurance programs facilitated through captive insurance companies. Transfer of cyber risks through captive insurers will drive growth in reinsurance markets for cyber insurance products, and may allow large insureds with unique cyber risk profiles to self manage underwriting and contractual uncertainties. Alternatively, many businesses may opt to include large self insured retentions for certain cyber risks placed through existing insurance markets in an effort to manage premium expenses.

Industry specific forms

Insurance markets have already begun to offer cyber insurance products tailored to cyber risks unique to specific industries, including the retail, energy, financial and professional services, technology, and healthcare sectors. A wide variety of businesses that rely upon automated equipment, such as utilities, industrial manufacturers, food processors, and agricultural businesses, will present different cyber risk profiles that may not be effectively transferred under existing insurance programs. In addition, manufacturers of connected consumer products, such as the manufacturers of automobiles, drones and other vehicles, may fuel demand for sector specific cyber insurance products to supplement or replace existing coverages.

Conclusion

The technologies creating cyber risks are evolving rapidly, and cyber insurance markets are adapting to keep pace with new risks. The coming years will most likely see an increased focus on adequately assessing and insuring cyber risks, resulting in innovative underwriting approaches to meet demands for increased capacity and coverage for new types of cyber risks.

NEWS IN BRIEF

UK initiative to assist firms in understanding cyber threats

The UK Chancellor of the Exchequer, Phillip Hammond, announced the creation of Industry 100, an initiative that invites private sector organisations to embed staff into the UK's National Cyber Security Centre ('NCSC') to develop a clearer understanding of cyber threats faced by the UK, at the official opening of the NCSC on 14 February 2017.

"Much of the critical infrastructure in the UK is in the private sector," said Andrew Moir, Partner and Head of Global Cyber Security at Herbert Smith Freehills LLP. Departments across the NCSC will identify roles, of which there will be 100 in total, where they require industry expertise and then post the relevant advertisements on the NCSC website, allowing organisations to apply to embed a person in these secondments as an 'integree.' "Given that the nature of threats to different industries can be very diverse, by seconding staff into the NCSC the Industry 100 aims to promote knowledge sharing both into and out of the NCSC to reduce cyber risk across the board," adds Moir.

Although only recently officially opened, the NCSC was launched in October 2016 and brings together the Centre for Cyber Assessment ('CCA'), Computer Emergency Response Team UK ('CERT-UK') and Communications-Electronics Security Group ('CESG'), GCHQ's information security arm. "Bringing all the various bodies together will enable a more focused approach to defending the UK from the ever-increasing cyber threat," believes Moir.

China aims to clarify review regime under security law

The Cyberspace Administration of China ('CAC') issued, on 4 February 2016, a draft of its Network Products and Services Security Review Measures ('Draft Measures'), further to the adoption of the Cyber Security Law ('Law') in November 2016, which is due to take effect from 1 June 2017. Under Article 35 of the Law, network products and network services procured by operators of critical information infrastructure network are subject to national security examination. The Draft Measures set out the implementation of this review regime.

Michelle Chan and Clarice Yue of Bird & Bird highlighted, "The Draft Measures bring clarity to the review regime [and] give guidance to operators of critical information infrastructure. Moreover, it is clarified that a new Network Security Examination Committee will be established to review important policies of network security examination, and a third party expert committee will also be set up to conduct integrated security assessment."

Despite the above, Chan and Yue note that there are still areas of the Draft Measures that lack clarity: "For example, the Draft Measures require that the departments in charge of 'key industries' are required to organise security examination of network products and services in accordance with the requirements of the national security examination, but the list of 'key industries' only includes financial, telecommunications and energy industries and does not appear consistent."