Global Cyber Newsletter

Q1
19

TransRe™
We value risk.

Welcome to our cyber newsletter. We hope you enjoy the articles and updates that our editors have put together.

The idea of war without physical fighting has been around since at least the 5th century BC. While countries and armies may still teach the same war strategies, it is clear that with technology and the internet, methods for attacks are changing, and now more than ever perhaps, enemies can be subdued without fighting.

"The supreme art of war is to subdue the enemy without fighting"

Sun Tzu, The Art of War

Before we discuss cyber-war and current litigation – a hot topic in the cyber insurance space (see page 5) – we offer a reminder on the NotPetya attack (2017), which offers a good case study on coverage.

If you have not already read it, we highly recommend Wired's article: The Untold Story of NotPetya, the Most Devastating Cyberattack in History. In this event, the NotPetya attack begins as an assault on one nation (Ukraine) by another (Russia), and features malware disguised as ransomware, deployed through servers from a commonly used accounting software company based on the Ukraine. The malware self-propagates, and while the Ukraine is hit especially hard, the virus spreads rapidly throughout the world within hours as well – affecting all types of industries: shipping, manufacturing, banking, law, construction, hospitals, airports, food production, and distribution, to name a few.

According to the article, the economic damages are $10B (with a portion of this figure picked up by insurers through cyber, all-risk property and kidnap and ransom policies). Because of this malware, computers and systems are "bricked", or rendered useless, resulting in business interruption. IT staff rushes to stop the problem from spreading, and then works as fast as possible to replace hardware and get systems back up and running.

While cyberwar is a term used throughout the article, no war is officially declared.

The current debate centers on this attack and the question of: should these losses be covered in insurance policies? The answer, as is often the case, is that it depends on the wording.

The policies denying coverage on NotPetya are all-risk property policies that, contrary to popular opinion, are not silent and in fact provide affirmative cyber coverage embedded within the policy – covering damage to data, programs or software caused by perils including viruses or malware. We still see this coverage offered today – typically with a sub-limit, and most often with business interruption included in the cap (after hard lessons from NotPetya where business interruption was not included in the sub-limit). The basis for denying coverage in the all-risk policies is due to very broad (and common) war exclusion language that excludes "hostile or war-like actions".

In contrast, the cyber-specific policies on NotPetya have different war exclusionary language and have not contested coverage (we note that war exclusionary language varies drastically in many types of policies).

The war exclusion therefore has hit center stage and many companies are now reviewing their war wordings to clarify scope and intent. We think this is overdue as the insurance industry wrote most war exclusions to respond to conventional attacks on tangible assets, long before the idea of cyber war.

An important consideration here is whether the insurance market has the capacity to handle a massive nation state attack / accumulation of exposure from cyber-war. To draft an effective war exclusion, intent of cover needs to be clear with consideration of the following:

- Does the war need to be declared, and by whom?;
  - A single nation state, or should there be a consensus agreement between multiple nations in the declaration of a cyberwar?
- Does the war need to be attributed to another nation state or….
- Does the war have to be targeted against specific states?
- Should indiscriminate targets / collateral damage be included in the definition of the war event?
- Should there be a dual trigger of size of loss and perceived or declared nation-state attack?

The courts will consider many of these questions related to intent in the current litigation, as the wording seems open to interpretation. In the Mondelez and Merck cases, the burden of proof is on the insurance companies to prove event exclusion due to war, based on the policy definition. Mondelez v. Zurich is being heard in the Circuit Court of Cook County, Illinois and the Merck case against multiple insurers is being heard in the Superior Court of New Jersey. Companies' risk managers and the (re)insurance world will be watching these cases closely.

Regardless of outcome, companies will have to contemplate their definition of and appetite for cyber-war and cyber conflict, and address wordings appropriately so that there is transparency in coverage.

The art of war continues to develop, but the principles very much remain the same.

Elizabeth Geary
Global Head of Cyber

TABLE OF CONTENTS

Notable Breaches PG 4

- Financial Sector
- Political Targets
- Business Interruption at large Aluminum Producer Due To Ransomware
- Millions of CVs Exposed In China
- Another Heath Data Breach In Singapore
- Commercial Operations Not Impacted In Cyberattacks on Major European Companies
- ASUS Computers Breached Via In-house Update Tool

Regulatory & Legislative Update PG 5

- Denied! Two Trailblazing Lawsuits Addressing Cyber War On Property Policies
- French Regulator Fines Google For Breaches Under GDPR
- Facebook
- Illinois Supreme Court Rules “Actual Harm” Not Necessary In Biometric Privacy Suit
- The UK’s Information & Financial Conduct Regulators Agree To Cooperate
- Dutch Regulator Considers Consent Under GDPR
- Yahoo Settles Derivative Lawsuit for $29M

Global Cyber Security PG 7

- Weather Apps Sued for Tracking Users
- Apps Aren’t The Only Ones: AT&T, T-Mobile, and Sprint Sell Users Location Data
- Amazon Ring Faces Scrutiny for Lack of Controls
- Finland Investigating Nokia Phones Sending Data to China

CryptoCorner PG 8

- CryptoExchange Death Costs Investors $135M
- Nearly $1B in Cryptocurrency Stolen in 2018
- 10 Year Prison Sentence for Cryptojacker

Cyber Reports PG 8

Guest Articles PG 9-14

- Spear Phishing, What Are You Going To Do?
- GDPR/Cyber Risks and Exposure to Fines & Penalties An English Law Perspective

NOTABLE BREACHES

Financial Sector
An attack on Malta's second largest bank, Bank of Valletta brought chaos to retailers when the bank was forced to take down cash machines, mobile banking and e-mail services following a cyberattack. The attack involved the transfer of €13m to international banks. The funds have been traced and the bank is seeking to have the transactions reversed. Customer accounts were not affected.

Banks in Australia have contacted customers regarding a breach linked to a property valuation firm, LandMark White. The firm is widely used by the largest banks in the country. Personal data of customers is said to have been discovered on the internet. Up to 100,000 customers may have been affected.

Political Targets
State actors are suspected in an attack launched against the computer systems of the Federal Parliament in Australia

Photograph: Lukas Coch/AAP

in the build up to national elections. The attack is reported to have targeted the system that houses lawmaker's official e-mail account but there is no evidence that it was intended to influence or disrupt electoral or political processes.

Hundreds of German politicians including Chancellor Angela Merkel have had sensitive data published online. Data is said to included personal phone numbers and addresses, internal party documents, credit card details and private chats. It is understood that a Twitter account began publishing the documents online in December in the form of an advent calendar. There was no evidence of the involvement of a foreign government. It is not clear whether this was an attack or a leak. Some reports suggest that data was obtained through improper use of login details to cloud services.

Indonesia confirmed that its voter database had been the subject of a series of probing attacks in the lead up to presidential and legislative elections in a bid to manipulate and modify content and create ghost voters. The attacks have been orchestrated both locally and abroad.

Business Interruption At Large Aluminium Producer Due To Ransomware
Norweigian aluminium producer Norsk Hydro was hit with a ransomware attack in mid-March that affected their entire global IT operation.. By the 27th March Norsk had four out of five business areas running at normal capacity with manual workarounds. Based on a high level evaluation, the preliminary estimated financial impact for the first full week following the attack was around NOK 300 - 350 m ($35m - $40m). Aluminium prices rose to a three-month high in the wake of the news. AIG lead the cyber policy.

Millions Of CVs Exposed In China
200 million Chinese people have had their CVs exposed online. The data included a wealth of personal details on the individuals including names, addresses and educational history. It is understood that the data was compiled from 'scraping' several Chinese job websites.

Another Heath Data Breach In Singapore
Confidential data of more than 14,000 people from Singapore's HIV Registry was stolen and leaked online in Singapore. Data is reported to have included names, addresses, HIV status and other medical information. An American national, previously jailed and deported for fraud and drug related offences, is accused of the malicious breach having had unauthorised access to the registry through his partner, a doctor who previously led the Ministry of Health's National Public Health Unit. The data related to 5,400 nationals and 8,800 foreigners plus 2,400 related contacts.

Personal details of 1.5 million patents of SingHealth was compromised in Singapore's worst breach of personal data in history last year. Earlier this year SingHealth and Integrated Health Information Systems were fined S$250,000 and S$750,000 respectively for the failure to make reasonable security arrangements to protect the person data following this incident.

Commercial Operations Not Impacted In Cyberattacks on Major European Companies
Aircraft manufacturer, Airbus confirmed that it had detected a cyber incident on its 'commercial aircraft business' information systems which resulted in unauthorised access to data. Commercial operation were unaffected but some data relating to its employees in Europe was accessed. The investigation is ongoing.

Leading French engineering consultancy Altran Technologies is reported to have been the victim of a malware attack in January. It is understood to have affected the company's operations in some European countries. Limited information has been released by the company but it confirmed that it has not identified any stolen data or instances of propagation of the incident to its clients.

Visma, a Norwegian firm providing business software products to more than 900,000 companies across Scandinavia, has been targeted in an attack linked to Chinese hackers. It is thought that the hackers were seeking access to commercially sensitive information although, there is no evidence that data was actually compromised.

The attack is said to have been part of a sustained campaign known as Cloudhopper specifically targeting technology service and software companies in order to reach their clients.

ASUS Computers Breached Via In-house Update Tool
At least 500,000 computers are understood to have been breached via a pre-installed update tool found on all ASUS machines, although it appears the bad actors were specifically targeting only about 600 of those systems. To date it is unknown whose systems were the ones being targeted. The breach was discovered in January by Kaspersky Lab, but has apparently been active for months.

REGULATORY & LEGISLATIVE UPDATE

Denied! Two Trailblazing Lawsuits Addressing Cyber War On Property Policies:

- Mondelez International v. Zurich American Ins. Co., Cir. Ct., Cook County, IL, No. 2018L011008. Mondelez filed suit after Zurich denied $100M in claimed losses resulting from the NotPetya incident, which allegedly bricked 1700 Mendelez servers and 24,000 laptops. Per the complaint, Zurich based the denial on the traditional "hostile and warlike action" exclusion commonly found in such policies.
- Merck & Co., Inc. v. ACE American Ins. Co., Super Ct., Union County, NJ, UNN-L-002682-18. In this suit, Merck sued insurers / reinsurers for declinations based on claims that the event precipitating the losses was "an act of war or terrorism."

The approach of the courts to the application of these clauses as they appear in more traditional lines of business and in the context of a cyber event will be monitored with interest.

French Regulator Fines Google For Breaches Under GDPR
French regulator, Commission Nationale de l'Informatique et des Libertés (CNIL) has issued a €50m penalty to Google for breaches of GDPR. The penalty follows complaints from two European rights groups, the Max Schrems' nonprofit group, None of Your Business (NOYB) and La Quadrature du Net (LQDN). Google collected user data to allow it to personalise and target its advertisements.

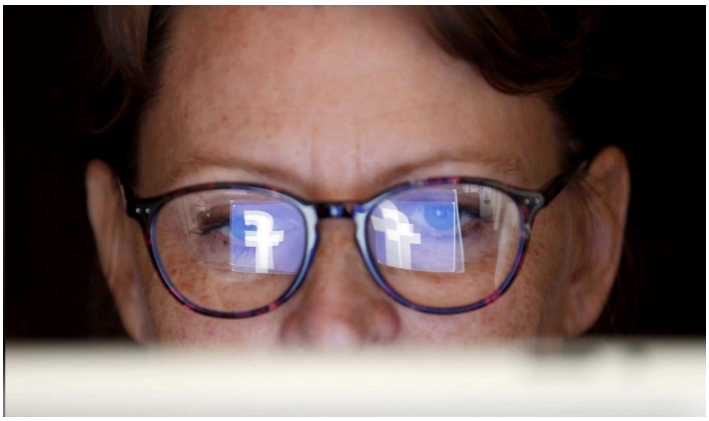
The regulator's principal concerns related to the lack of transparency, inadequate information and, therefore, a lack of valid consent while citing the scale and intrusiveness of the processing operations. The purpose of the processing was described in vague and generic terms and was excessively disseminated across several documents making it difficult for the user to understand the legal basis for the processing. As such, any consent given was not given on a sufficiently informed basis.

The European Data Protection Board (EDPB) has provided its first overview on the implantation of GDPR and confirmed that cooperation and consistency between national Supervisory Authorities (SAs) is working 'quite well'. Consistent application of GDPR is one of the primary roles of the EDPB. It acknowledges that the additional cooperation duties has increased the workload of SAs with an impact on the budget of the regulators. EDPB reports a total of 206,326 case of which 94,622 were complaints, 64,684 data breach notifications with another 47,020 falling into a category of 'other'. Fines issued by SAs total €55,955,871 of which the Google fine mentioned above will represent the majority.

Separately, the European Commission fined Google €1.49B for breaching antitrust rules. This represents the third year in a row that Google has faced a large European fine after the record €4.3B fine last year for abusing its market dominance in mobile, and €2.4B in 2017 for manipulating shopping search results. Both the previous fines are being appealed.

Facebook

In a landmark ruling following a 3 year probe, the Federal Cartel Office of Germany, has given Facebook twelve months to curb the unrestricted collection and use of data without consent. The competition regulator considered that the social media giant abused its market dominance. It particularly objected to how Facebook was pooling data on individuals from third party apps and online tracking of people through 'like' or 'share' buttons who may not have even been members. The regulator is seeking to stop Facebook forcing users to agree to unrestricted collection of data and assigning non-Facebook data to their Facebook accounts. Facebook is considering an appeal stating that the regulator



REUETERS/Regis Duvignau/Illustration

had underestimated the level of competition in Germany and that it was encroaching into areas that should be handled by data protection watchdogs.

Facebook's recent announcement to integrate its 3 social media platforms including Instagram & WhatsApp has drawn the attention of the Irish Data Protection Commission (DPC) which has requested an urgent briefing with the company. A particular focus of the DPC will be the sharing and merging of personal data between the Facebook companies. Prior proposals to share data between platforms has given rise to significant data protections concerns.

Meanwhile in America, Facebook has faced criticism for paying people to install a "Facebook Research" VPN that decrypts and analyses all data on the users phone. Facebook is specifically targeting children as young as 13 with this program. After the discovery and revelation of the program by TechCrunch, Facebook announced they would shut the IOS version of the app down. Apple responded by banning the Facebook VPN from the App Store. This despite Facebook Founder and CEO Mark Zuckerberg's elaborate pledge to pivot towards privacy, which was penned in early March. The pledge elicited some significant commentary on Facebook's future, at a time when the company is already facing a criminal probe for their handling and sale of user data.

Illinois Supreme Court Rules "Actual Harm" Not Necessary In Biometric Privacy Suit

In the case Rosenbach v. Six Flags, the IL Supreme Court found that a "mere" statutory violation is sufficient to show that a person is aggrieved under the terms of the Illinois Biometric Information Privacy Act (BIPA) – a first-of-its-kind ruling for a first-of-its-kind law. In this case, the plaintiff alleged that theme park Six Flags collected her son's thumbprint without permission, in violation of BIPA. Under this ruling there need not be any additional allegation that the data was stolen or misused. There are now hundreds such lawsuits already filed on the basis of these "technical violations" of BIPA, with many warning of a flood to come.

The UK's Information & Financial Conduct Regulators Agree To Cooperate

The UK regulators, the Information Commissioner's Office (ICO) and the Financial Conduct Authority (FCA) have agreed a memorandum of understanding (MoU) as regards future cooperation, coordination and information sharing to enhance their abilities to exercise their respective functions. The MoU recognises that there are areas in which there are complementary functions between the regulators and powers for which the most appropriate body or bodies will commence and lead the investigation.

Meanwhile, the UK's Prudential Regulation Authority (PRA) has provided further feedback to CEOs of general insurance firms to its 2017 supervisory statement on 'Cyber insurance underwriting risk'. The regulator has concluded, following further consultation with firms that more can be done to ensure the prudent management of cyber risk exposures. In particular, it considered that quantitative assessments of non-affirmative cyber risk are not well-developed. The regulator also noted the material widening of coverage for affirmative cyber risk with obvious prudential risks for insurers if not accompanied by appropriate pricing adjustments and adequate risk management.

Dutch Regulator Considers Consent Under GDPR

The Dutch Data Protection Authority (Autoriteit Persoonsgegevens) recently published guidance on the requirement for consent to be 'freely given' under GDPR. The issue arose following complaints relating to the usage of cookie walls which prevent the user from accessing a website without consenting to the use of tracking cookies. The regulator confirmed that such practice was not consistent with GDPR. Article 7(4) of GDPR provides: "When assessing whether consent is freely given, utmost account shall be taken of whether… the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

Yahoo Settles Derivative Lawsuit For $29M

In 2013 – 2016, Yahoo was a common name in the cyber world after a series of breaches compromised the user data for three billion Yahoo users. Now, in what is possibly the first example of a successful shareholder suit against the Directors and Officers of a breached company, a $29M settlement was approved in January. Notably, the allegations concerned the lack of proper cybersecurity oversight by the defendants – the risk there had the shareholders prevailed at trial would have been the establishment of baseline that a board can be liable for a lack of cyber-oversight.

REUETERS/Regis Duvignau/Illustration

- Meanwhile, the class action lawsuit by aggrieved users continues: also in January, the judge rejected a $50M proposed settlement, saying Yahoo failed to disclose adequate details of the settlement costs and fund, without which a full evaluation of the adequacy of the proposed settlement could not be made.

GLOBAL CYBER SECURITY

Weather Apps Sued For Tracking Users

In a story that should surprise no one after reading the New York Times report referenced in the Global Cyber Security section of our last newsletter, The Weather Channel has been sued by the City of Los Angeles for inappropriate use of location data. The lawsuit claims that The Weather Channel app mines location data, which is then monetized and sold to IBM affiliates and other third parties for commercial purposes. This after another popular weather app, Accuweather was caught similarly monetizing users location information in 2017, capturing that information even when location sharing is turned off.

Apps Aren't The Only Ones: AT&T, T-Mobile, And Sprint Sell Users Location Data

A Motherboard investigation recently found that several large telecoms were selling real-time location data of their users. This type of real-time location data is a step beyond the "usual" data mining-monetization: for $300, real time location data on specific users was widely available, and in some cases was sold to bounty hunters on the black market.

Similarly, another swath of apps have been found to record every keystroke and everything shown on a phones screen – all without user knowledge. Such apps include: Air Canada, Hollister, and Expedia. Apple

Amazon Ring Faces Scrutiny for Lack of Controls

The Ring video monitoring suite of devices – recently purchased by Amazon – bills itself as a convenient security feature of the modern home, but investigation has revealed that their own internal security practices leave much to be desired. A folder hosted on Amazon cloud storage – unencrypted – held ever recording from every Ring camera anywhere in the world. Additionally, a multitude of executives and engineers were given credentials that allowed them to access users cameras' live feed at any time, even when such unfettered access was wholly unnecessary for their jobs.

Finland Investigating Nokia Phones Sending Data to China

The Finnish data protection ombudsman is investigating a possible breach of data protection rules after Nokia phones were found to be sending unencrypted data to a Chinese server – a set of facts very similar to recent U.S. accusations against Huawei. The manufacturer of the Nokia phones has claimed that no PII was transmitted and the transmissions were the result of a software error.

CRYPTO CORNER

CryptoExchange Death Costs Investors $135M

In early 2019, the founder of Canadian-based CryptoExchange Quadiga died unexpectedly – leaving all funds stored on the exchange completely unretrievable, as he is thought to have held the only access key. The funds were held in "cold storage" – essentially, offline, to protect against theft – on the founders' encrypted laptop, which he alone has the access codes for. In an unfortunate twist for investors, subsequent investigation revealed the only known Quadriga "cold wallets" had been emptied nearly a year earlier, adding additional uncertainty to where the money had gone.

Nearly $1B in Cryptocurrency Stolen in 2018

Cryptocurrency theft jumped 3.5 times over 2017, to a staggering total of $927M in 2018. Although some of the larger, more sophisticated cryptocurrency exchanges have been able to secure insurance, the bulk of the market is simply unable to access the limited capacity in the marketplace.

10 Year Prison Sentence for Cryptojacker

A college student who allegedly stole more than $5M in cryptocurrency through a method known as SIM highjacking accepted a plea deal that will put him in a California prison for 10 years.

Cyber Reports

Aon – 2019 Cybersecurity Risk Report

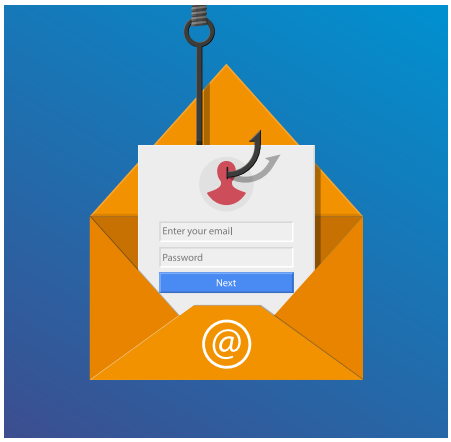
Mayer Brown – 2019 Outlook: Cybersecurity and Data Privacy

Pew Research Center conducted a study of what people view as the chief risks – global warming is the current number one, but Cyberattacks has risen to the third spot behind only global warning and ISIS.

Beazley - Beazley Breach Briefing

Spear Phishing, What Are You Going To Do?

By Neil Inskip VP, IT Manager



For years now, we've been getting emails from foreign Princes saying they'll give us their entire estate, for a small bank transfer, we didn't fall for them the first time and we still don't. Back in the early days phishes were no better than those "419 Advance Fees scams" - 419 being the criminal code in Africa that covers the offence, very easy to spot and ignore. The majority were also from poorer nations, some from intelligent students who could not find work, who found it easy to get an old PC and a modem and send many emails simultaneously. They lacked grammar, had poor spelling and at risk of sounding like Neville Chamberlain came from "a faraway country of which we know nothing". Nowadays the "crime war" has begun and there is big money involved. This quarter I'll be looking at Phishing and what IT departments can do to help.

Anti-spam software goes someway to helping, using a set of heuristics to analyse every inbound email, looking for the words like "Cheap Rolex", "Legal Highs", etc and possibly by checking against a central cloud database of known spam messages and senders. Companies that use cloud based anti-spam solutions stop millions of spam emails for their users each month, but some still get calls to the helpdesk to say one got through. Why is that? The answer is simple, make the email as much like a business worthy email as you can, then you must let it through, either that or lockup our system so much you really can't communicate with the outside world. How do you make it feel like a business email? Possibly you can hack into a business who trades with other businesses and then study their email transactions and the language they use, then phish their customers or dumpster-dive their rubbish and get hardcopy emails, there is no real secret except research.

Systems are wonderful things, but the key is user education. As a universal scenario we can all relate to, I can better you wish to purchase seen and agreed a small amount, let's say back and forth, the car payment instructions. car dealers do not but let's assume they illustrate the problem. Let's say a used car that you've already price on, the value is not a $25,000. After a few emails dealer emails you their bank Certainly, here in the UK used always have a great reputation, are an honest company and we'll also assume the dealership is not a massive franchise, just a small three-man team.

"Indeed, the larger the company the bigger the potential criminal returns"

The question is, how much security do you think they have to protect their email system? Follow on questions could be, is their email account password set to "password" or do they have insecure WI-FI access connected to their email server? Unless you confirmed the payment instructions with the dealer you know over the phone or in person, can you be 100% sure you just made payment to the right bank account?"

Clearly the reverse could be true, they could have excellent IT security and it's not just the small companies, any "chink in the armour", anywhere, can be exploited. Indeed, the larger the company the bigger the potential criminal returns.

So, once we realise the emails are too clever it becomes education around process as well as the normal checks around spelling, grammar and making sure the email is from an un-spoofed domain, “AcmeCorp.com” can so easily be spoofed with “Acme-Corp.com”. Shredding your paper waste is also another requirement in a long list of security best practices.

For IT departments the only real metric you can gather around the effectiveness of your “User Ed” is to generate your own spam, log how many people click on it, then deliver on demand training to those people who fall for the trap. Usually some red faces and interesting stories emerge around why they fell for it come to light, but it’s a continual process.

I am a firm believer in going the whole way to providing a comprehensive awareness program, not quite t-shirt campaigns, but if you stick up a poster next to the water cooler about “The use of Strong Passwords”, if as little as one person takes notice that’s one person you don’t need to worry about, as much anyway.
Guest Article

GDPR/Cyber Risks and Exposure to Fines & Penalties An English Law Perspective

The commercial world is aware that the new GDPR regime within the UK and EU came into force in May 2018 and imposed new data privacy and consent requirements on the use and retention of data.

These requirements brought into play compliance and governance issues breaches of which are to be enforced with a significant new level of fines, being up to Euros 20m or 4% of global turnover whichever is the greater amount.

From a data protection and GDPR perspective these level of fines are significant and of major concern to the commercial community. The regime for imposing fines is set out in Article 83(i) of GDPR which states that "the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive". This is quite a broad regulatory regime for imposing administrative fines, and use of the word "dissuasive" implies an element of deterrence. When imposing a fine the regulatory authority shall have regard to a range of factors including the nature, gravity and duration of the breach and the extent of any damage suffered, and action taken to mitigate the damage. Recent high profile fines imposed by the ICO involve Facebook and Equifax for data breaches for which they were fined £500,000 each, along with the high profile fine of Tesco Bank (£16.4m) imposed by the FCA.

It is against this background, and since May 2018 that the prospect of the commercial community receiving fines for breaches of their data/GDPR obligations has been driving recent interest amongst insureds and brokers of the possibility of obtaining insurance for fines and penalties, arising from breaches of data requirements. Thus the interest in expanding cyber policies within the London market to include an indemnity for fines and penalties. The question is – is this possible?

From an English law perspective, the possibility of fines or penalties being capable of being insured is an issue that has been developed by the common law over the last 200 years or so, and has developed from the principle of ex turpi causa. Common law has developed and applied the principle of "ex turpi causa" into what is commonly referred to as the "illegality defence" i.e. broadly speaking a claim based upon a criminal or illegal act will fail. "No Court will lend its aid to a main who founds his cause of action upon an immoral or illegal act". This common law principle has developed over the years and as a consequence insurance cover is not available for fines or penalties arising from criminal or illegal/wrongful acts, this being contrary to both common law principles, and public policy.

The modern principles of ex turpi causa under English common law were recently confirmed in the Stone & Rolls v Moore Stephens [2009] case. The case concerned a "one man" company which was defrauded by its director. The House of Lords struck out a claim by the company's liquidator against the company's auditors alleging that the auditors negligently failed to alert the company to the director's fraud. The House of Lords held that the director was to be treated as the company's sole mind, will and beneficial owner and therefore his dishonesty was to be attributed to the company. As a result the liquidator could not bring the claim. The House of Lords restated the principles of ex turpi causa with one legal principle being that the Court will not assist a Claimant to recover a benefit from his own wrongdoing.

This was simply restating the common law position, and is another expression of the basis of whether fines or penalties are insurable. Common law will not permit insureds to "recover a benefit" from their own wrongdoing by obtaining an indemnity for any fines or penalties that have been imposed upon them arising from their wrongful conduct, criminal activity or illegal conduct.

The English Court had another opportunity to look at the issues and application of the ex turpi causa principles in the Safeway v Twigger Commercial Court and Court of Appeal hearings [in 2010]. The issues which were subject to judicial comment have general application to the recoverability of fines and penalties and in the particular circumstances of this case, on whether OFT (Office of Fair Trading) financial penalties would be insurable at law. This case

involved serious breaches of the Competition Act arising from a cartel of supermarkets that were fixing the price of milk and dairy products. Safeway were subject to a fine of £10.7m as a result of their conduct. During the Commercial Court hearing the Judge took the view that the anti-competitive conduct of Safeway "involved the necessary element of moral reprehensibility or turpitude and are sufficiently serious to engage the ex turpi causa rule in principle"; thus indicating that the conduct of the various directors and officers involved in the anti-competitive conduct was sufficiently serious. The Court also held that the OFT proceedings and penalties were of a quasi criminal nature. As a result the penalty imposed by the OFT, although regarded as being of a civil or administrative nature, had the characteristics of a fine imposed for the commission of a criminal offence (i.e. being punishment/deterrence rather than compensation).

In these proceedings, Safeway were seeking to recover from their culpable directors and senior officers for subjecting the company to its involvement in the cartel and the subsequent penalty. When the case reached the Court of Appeal, the judicial view was that passing on these damages to the individuals who were responsible for the illegal conduct was not possible because of the particular wording and provisions of the Competition Act. It was

this appellate decision that prevented Safeway from seeking to recover from the culpable directors/officers and which relieved any D&O insurers of having to decide whether they could indemnify the directors and officers for Safeway's claim for damages arising from the OFT fine and the serious misconduct of the culpable directors and officers. As Safeway could not pass this onto the culpable directors, this issue did not arise. However, the Safeway case provides a good steer as to how this issue is to be approached by insurers and the test of culpable conduct to be applied in the future from an insurance perspective.

In other parts of the commercial regulatory market, it is widely accepted that fines and penalties for breaches of regulations and obligations are not capable of being insured, such as Health and Safety breaches and fines imposed upon companies and individuals. These are not insurable as a matter of public policy as well as common law principles. The same principles apply to environmental regulations and DEFRA requirements relating to environmental breaches and liabilities and fines. The FCA has its own particular prohibition arising from FSMA 2000 which prohibits "entering into or payment under, a contract of insurance in respect of financial penalties", thus specifically preventing firms or individuals who are fined for various breaches of FSMA 2000 requirements, from seeking insurance cover.

It is not just an issue of fines/penalties that arise from serious wrongdoing that are relevant. The growth in the number of civil/regulatory requirements and their breach further complicates this issue as some of the breaches could arise from minor administrative breaches of an unintentional/innocent nature and there being no element of wrongdoing on the part of the company or its staff. In such circumstances, the issue arises of whether such minor breaches are capable of being insured, and realistically the position is uncertain at the present time. Thus Insurers should proceed on the basis of the current common law principles that the indemnity of fines and penalties is not permissible under English law.

However any civil/regulatory fines and the circumstances under which they were imposed will need to be looked at so as to determine the nature of the breach and investigation and whether it was of a "quasi criminal" nature, and how culpable was the behaviour of the company or its senior management. Ivf the company's behaviour is serious and liable for a fine and arises from wrongful conduct by its directors and officers, then the circumstances will be entering the territory of ex turpi causa, rather than being the circumstances of being fined for minor/innocent administrative breaches. Within the data breach/GDPR scenario, underwriters will need to look at issues of serious misconduct and possible criminal/quasi criminal conduct, even if this has arisen within the scenario of a civil/regulatory breach and wrongdoing. This will mean that the test for serious misconduct/ex turpi causa will need to be applied to determine the nature of the breach.

The UK insurance sector along with the London insurance market maintain the view that "fines and penalties" are not insurable, and one only needs to look at various consumer policies which do not provide for the recoverability of fines and penalties, and this prohibition extends to commercial policies. However indemnities for fines and penalties, in certain circumstances, are beginning to creep in to wordings in the FI and D&O sector as well as certain PI and Cyber policies and underwriters need to be careful. As was indicated previously in this article, it is the recent interest in cyber policies giving wider coverage that is currently driving a need to seek insurance for fines. Amongst the various wordings that are available, the ones that state that some level of fines/penalty recovery is available "if permitted by law"

or “if insurable at law” is probably the safest bet for underwriters given the need of insureds and brokers to have some form of cover from fines and penalties, although it also allows underwriters to hedge their bets on whether the fine and the circumstances giving rise to it is actually capable of being indemnified. However the most obvious way of dealing with the issue and so as to avoid any disputes in the future, is for underwriters to maintain their position that fines and penalties are not insurable.

That is the position under English law, although it is accepted and recognised that in various other jurisdictions such cover is permissible, for certain of fines/penalties that are imposed in certain circumstances.

About Francis

Francis’s practice and experience covers a wide range of insurance and reinsurance sectors, mainly dealing with dispute, advice and coverage issues, with particular experience in energy, professional indemnity, political risks/contract frustration, commercial property, financial institutions/D&O, pharmaceutical/product liability, contingency risks, binding authorities, a range of reinsurances such as marine excess of loss market and MGA’s. Over the years he has been involved in a wide range of contractual disputes involving these types of insurances/reinsurances.

Over the years Francis has been involved in some of the most important and significant insurance and reinsurance cases and authorities that have been decided either by arbitration or the London Commercial Court.

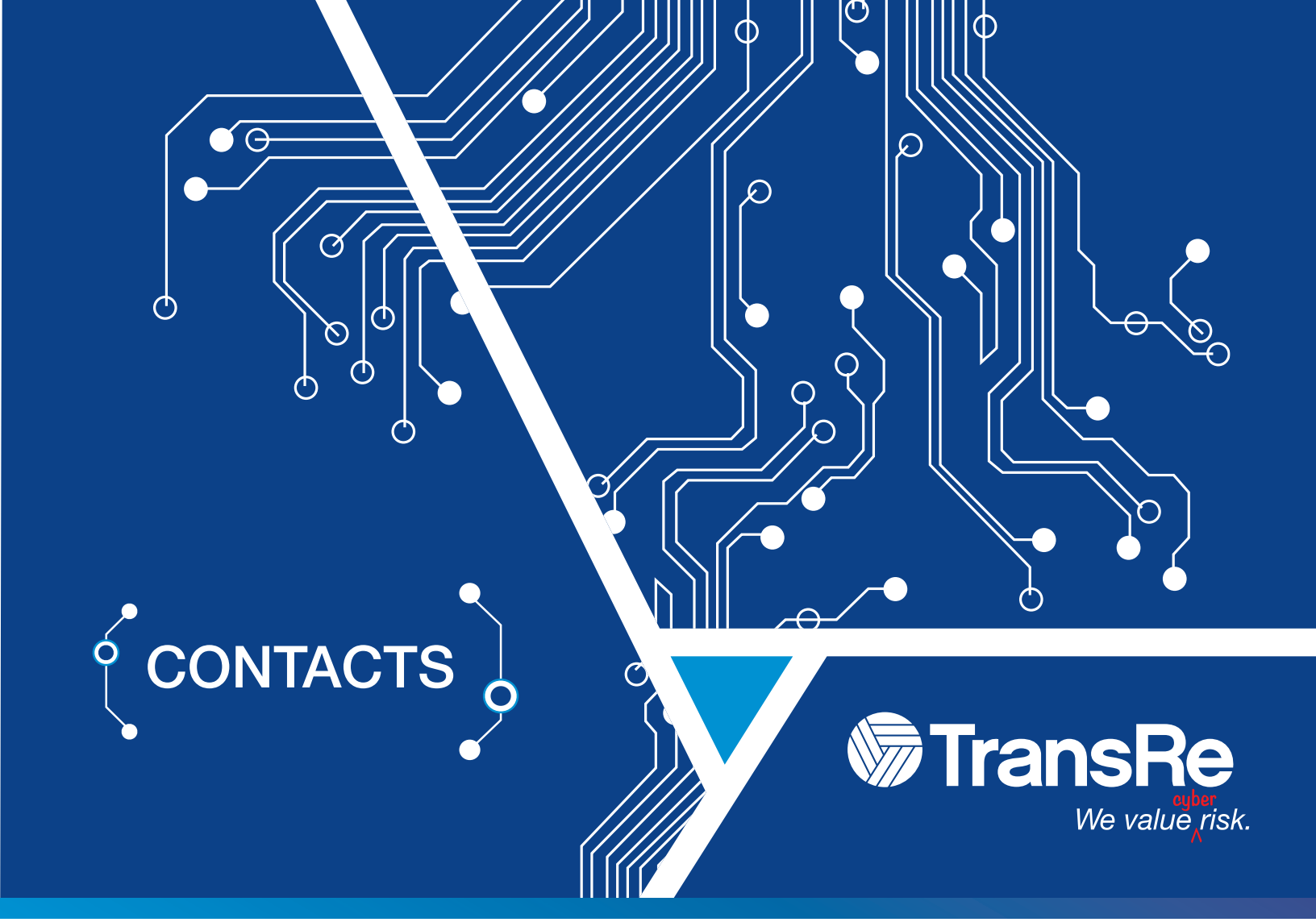
Francis is listed in ‘Chambers & Partners’, ‘The International Who’s Who of Insurance & Reinsurance Lawyers’, ‘Super Lawyers’ and ‘Best Lawyers in the United Kingdom for Insurance Law work’.

TransRe
We value risk.

TransRe is a leading international reinsurance organization with a global reach and local decision making.

Our relationships are based on years of trust and experience. We have a flat organization structure that carries our A+ capital rated ability with our proven willingness to pay claims.

We proudly take a hands-on approach and write every product in every jurisdiction with a promise not to compete with our customers.



Editors

Calum Kennedy
Vice President
44 (0) 20 7204 8645
ckennedy@transre.com

Peter Cridland
Assistant Vice President
1.212.365.2032
pcridland@transre.com

Phylip Jones
Global Marketing Manager
1.212.365.2281
pjones@transre.com

Lauren Markowski
Cyber Risk Underwriter
1.212.365.2301
lmarkowski@transre.com

Rhett Hewitt
Cyber Risk Underwriter
44 (0)20 7204 8676
rhewitt@transre.com

Miguel Canals
Cyber Risk Underwriter
1.212.365.2266
mcanals@transre.com

Elizabeth Geary
Global Head of Cyber Risk
1.212.365.2243
egeary@transre.com

Alex Bustillo
Cyber Risk Underwriter
1.212.365.2376
abustillo@transre.com