TransRe
We value risk.

Global Cyber
Newsletter
4Q2017

TransRe cyber
We value risk.

Table of Contents

Notable Cyber Breaches & Threats

PayPal Acquisition Breached, 1.6M Users Exposed

Ongoing, unauthorized access by unknown parties exposed the personal information of 1.6M people. The breach likely could have been worse had the acquired companies' systems been integrated into the PayPal system, but that step had not yet been taken when the breach was discovered. PayPal acquired a payment processing company in July 2017.

Financial Impact of Nuance Breach Continues

Healthcare transcription service Nuance was breached in a June 2017 NotPetya attack, but the financial impacts continue to reverberate, negatively impacting Q4 financials by $53M. Total financial impact from production downtime and customer credits is estimated at $68M.

Canadian Hospital Suffers Breach

Approximately 11,000 patients from Brampton Civic Hospital in Ontario received notification that their medical records were breached. It appears that an employee of the hospital accessed patient medical records and ordered unauthorized medications to their accounts. Few details are available, but the person responsible has been criminally charged.

Uber Breach

Uber concealed a 2016 data breach that affected 57 million Uber users and drivers across the globe including the US, Canada and the UK. It is also understood to have paid the hacker for $100,000 ransom for the destruction of the stolen data. The company found itself in regulatory hot water for its failure to disclose the in jurisdictions where breach notification is mandatory.

Cryptocurrencies Targeted

Slovenian cryptocurrency mining site, NiceHash has apologized after 4,700 bitcoin were stolen by hackers. The attacker infiltrated the company's systems through a compromised computer. Operations were suspended for 24 hours. The attack comes as the value of Bitcoin has soared to over $16,000.

Separately, over $30m worth of tokens were stolen through an attack on Tether's treasury wallets by hackers. The Hong based company is alternative to Bitcoin which is linked to the US Dollar.

Barclays Bank in Security Breach

The UK bank, Barclays has admitted that technical problems resulted in thousands of letters containing Personal Identification Numbers (PIN) being sent out in the post at the same time as new debit cards. The bank had to send new cards & numbers to customers. The bank advised that the issue affected less than 1% of customers.

Australian Government Department Warns on 2016 Data Breach

Credit card information, employee names, user names, work phone/e-mail addresses & system passwords were included in data stolen in a breach at the Australian Government Department of Social Services in a 2016 breach. 8,500 current and former employees have been warned that their personal data was compromised. There is no evidence that the data has been used for criminal purposes.

46.2 Million Mobile Subscribers Exposed in Malaysia

Personal details of most of the population of Malaysia have been posted online and offered for sale following a massive data breach in 2014. The data included home addresses, identity card numbers and SIM card information. All the major mobile operators were affected by the breach. Personal data from the Malaysian Medical Council; the Malaysian Medical Association and the Malaysian Dental Association was taken. The Malaysian government is working with carriers and police to investigate the issue.

Bank Cyber Heist in Taiwan

Far Eastern International Bank has been fined TWD 8 million by the Taiwanese financial regulator following a reported hack which stole $60 million in October. The majority of the funds were actually recovered. The hacker planted malware on the bank's servers and sent unauthorized doctored messages through the interbank SWIFT network. Two suspects were arrested in Sri Lanka.

Regulatory & Legislative Update

2017 Amendments to U.S. State Data Breach Laws

2017 saw the continued expansion of existing state laws, that set forth the responsibilities of breached party. Several states (Maryland, Delaware, Tennessee) expanded their definitions of “personal information”, and several states added a specific number of days within which notification must be made. The trend continues to be broader application through expanded definitions, more requirements of Attorney General notification, and more specific and shorter timelines for notification. Further, 2017 saw the enacting of the 47th state law, leaving only Alabama and South Dakota without such legislation.

Cottage Health System Settles State Regulatory Action

California hospital system Cottage Health agreed to pay a $2M settlement to resolve an investigation by the State Attorney General. The settlement covers two incidents, one stretching from 2011- 2013 in which 50k patient records were breached; the second discovered in 2015 involving 5k records. Both times the records were publically available and not behind a firewall due to the misconfiguration of a hospital server. The settlement also requires various IT security steps be undertaken by Cottage Health.

21st Century Oncology Agrees to $2.3M Fine. Additional Penalties

Although 21st Century Oncology is in bankruptcy, it continues to operate across 17 states and has reached settlements to resolve several outstanding issues and proceed in restructuring. The group will pay a $2.3M fine to the U.S. Dept. of Health and Human Services for the 2015 data breach that exposed the records of over 2.2M patients. Further, the affected patients will be permitted to pursue and recover reimbursement directly from 21st Century’s cyber insurer. Related court documents indicate there is roughly $4.2M remaining on that policy.

Privacy Shield... One Year On

A year on from the European Commission’s declaration that Privacy Shield was adequate for the purposes of EU data protection law, the framework has been reviewed by representatives of both the European Commission (EC) and the US Department of Commerce.

Privacy Shield is the successor mechanism to Safe Harbor which was deemed inadequate by the European Court of Justice in October 2015. Privacy Shield is a self-certifying program requiring a public commitment to the frameworks requirements. Over two thousand organizations have signed up to Privacy Shield to date.

The EC confirmed that the US authorities had put in place the necessary structures and procedures to ensure the correct handling of enforcement procedures and that cooperation with EU had stepped up. There were a number of recommendations for improvement including more proactive and regular monitoring of companies' compliance with the framework; More awareness-raising for EU individuals on how to exercise rights under Privacy Shield; closer cooperation between privacy enforcers and the appointment of a permanent privacy shield ombudsperson.

The European data protection watchdog, the Article 29 Working Party has threatened a legal challenge to Privacy Shield relating to, among other concerns, the access to data by the US authorities for national security and law enforcement. Similarly, the civil and human rights group, Digital Rights Ireland has challenged the EU's adoption of the Privacy Shield before the Court of Justice of the European Union on the grounds that it does not provide adequate privacy protection.

Growing Concern Over Kaspersky

The National Cyber Security Centre (NCSC) has advised the UK government not to use antivirus software from Moscow-based firm Kaspersky. In particular, where it is assessed that access to the information by the Russian state would be a risk to national security; a Russian anti-virus provider should not be chosen. The NCSC is working with Kaspersky to develop an independently verifiable framework to prevent UK data falling into the hands of the Russian state.

British bank, Barclays responded to the concern by notifying its customers that it was discontinuing an offer for free Kaspersky software for users of its online banking service.

In the US, President Trump signed legislation that bans the use of Kaspersky anti-virus software by federal agencies amid spying fears by the Moscow based firm. The move reinforces a directive issued by the administration in September that civilian agencies remove Kaspersky software. The software firm denies that it has links to any government.

Fines & Penalties

The Personal Data Protection Commission of Singapore (PDPC) fines digital marketing company. Social Metric Pte Ltd S$18,000 for unauthorized disclosure of personal data; the firm conducted social media marketing campaigns containing personal data of its clients' customers but failed to remove the information when the campaign was over.

Global Cyber Security

New Research Suggests Hundreds of Popular Websites Record Keystrokes

Princeton University released the first part of a multi-part series on IT issues, revealing that hundreds of popular websites use scripts to track the keystrokes of every visitor to the site, and then sends that data to third-party servers. There is no guarantee that these records of each website visit are – or could ever be – truly anonymized, as some privacy polices suggest. The websites for Bonobos, Wordpress, Microsoft, Norton, Fidelity, and many others are all included on the full list.

Bitcoin: Bullish Investment / Bearish Currency

Bitcoin value has continued its meteoric rise – starting the year at $997.69 per bitcoin, and reaching as high as $19,343.04 on December 16th. As promised futures trading of Bitcoin has begun, checking off another hallmark of an established investment vehicle. However, as discussed by TransRe's Peter Cridland in the PLUS webinar "Frontier of Cyber Risk and Litigation" on August 23rd, the utility of Bitcoin as a currency has fallen in nearly equal measure. Steam (among others) has announced it will no longer accept Bitcoin as a method of payment. Further, the hugely increased visibility of Bitcoin has attracted governmental attention: the UK and the EU now plan to introduce legislation aimed at requiring Bitcoin users to use their real names rather than online aliases to bring it in line with general currency and financial regulations. In the U.S., the Internal Revenue Service successfully obtained a court order requiring a large cryptocurrency exchange to turn over records for 14,000 customers. The action was taken by the IRS after "just 800-900 taxpayers reported bitcoin gains [on their taxes] from 2013 to 2015…"

Elsewhere in Cryptocurrency…

At least $150M in rival cryptocurrency Ethereum was likely permanently lost when a coder "accidently" locked down a number of multisignature wallets. Although the currency still exists, the owners cannot access it without Ethereum taking extreme measures that might end up undermining the very security of the currency. As Initial Coin Offerings ("ICO" – the cryptocurrency equivalent of a stocks IPO) have continued to make news, prompting the U.S. Securities and Exchange Commission to issue a statement cautioning investors against a "substantial risk of thefts or loss" in participating in them. To wit, cryptocurrency startup Confido disappeared overnight after collecting $375k in their ICO, prompting many to conclude it was a scam from the beginning. Meanwhile, Venezuela announced their intent to create their own "cryptocurrency" as an end-run around U.S. financial sanctions.

Guest Column

Is "Any One Event" Language Fit for Purpose When it Comes to Cyber Aggregation?

By Adam Strong, Partner HFW

Cyber aggregation is currently a hot topic. Numerous articles have been written highlighting the risks of cyber aggregation and how difficult it is to model accurately. Cyber is unlike any other peril and comparisons have been drawn with other systemic issues facing the insurance industry such as climate change. Some leading insurance market figures have suggested that cyber is, in reality, simply too big to insure and it should be a matter for the State.

There is also increasing pressure on cyber underwriters (both direct and reinsurance) to move away from the relatively well understood data breach response products and to provide wider and wider cyber protections that include, amongst other covers, physical damage and business interruption arising out of any cyber incident. In addition, there is the risk of silent cyber, namely, through lack of a relevant cyber exclusion (or a poorly drafted exclusion), cyber cover may accidently be granted in a policy that was never intended to provide it. If an insurer or reinsurer does not know that they are providing cyber cover then understandably they are not going to be giving any thought to the aggregation risk. Even in situations in which cyber cover is consciously included there is a general concern that proper thought is not being given to the risk of aggregation. A good and often quoted example of this is the extent to which cyber insureds use the same cloud service provider. If under the cyber policy vendor cover is provided and that service provider is attacked this can significantly magnify the risk.

However, notwithstanding the number of articles that have been written on the topic of cyber aggregation very little attention, if any, has been given to the language in the policy that provides for aggregation and whether this language is appropriate or what this language means in practice. The purpose of this article is to consider how the "event" language that is typically found in most reinsurance treaties governed by English law applies to cyber and whether further thought needs to be given to its use.

What Does "Event" Mean as a Matter of English Law?

A typical aggregation provision in a reinsurance treaty will state as follows:

'Loss" under this Contract means loss, damage, liability or expense or a series thereof arising from one event." [emphasis added]

Under such a clause a number of separate and distinct losses or claims can be aggregated if the reinsured or the reinsurer (it must be remembered that aggregation can work in either party's favour) can show that they all arise out of the same event. The word "event" is not typically defined in the relevant contract but has now been considered on numerous occasions by the English Courts and a fairly consistent body of case law has emerged. It is possible to draw the following conclusions from the case law as regards what amounts to an "event" and what is required to be able to aggregate.

1. What has happened must be capable of being described as an event. In Axa Reinsurance (UK) Plc v Field [1996] 3 All E.R. 517, Lord Mustill said that "in ordinary speech, an event is something that happens at a particular time, at a particular place and in a particular way". In other words, something identifiable and specific must have occurred. A general state of affairs, such as a global recession or a state of war between two countries, cannot be an event.
2. The losses that have occurred must be sufficiently closely connected with each other to be said to arise from one event. In considering whether they are sufficiently closely connected, the courts apply what is known as the unities test. The unities comprise time, location, cause and (in the case of human involvement) motive.
3. There must be sufficient causal connection between the event and the losses for the losses to be said to "arise out of" the event. The event does not need to be the proximate cause of the losses. A weaker causation connection is permitted but the event must still be a significant cause. If the losses are too remote then they cannot be said to "arise out of" the event.
4. In assessing whether individual losses can be aggregated as a single event the matter must be carefully scrutinised from the perspective of an informed observer in the position of the insured. The analysis is to be made analytically but also as a matter of intuition and common sense.

Whilst the principles surrounding event aggregation are relatively well settled and easy to state, the application of the principles to any given set of facts is one of the most difficult and academically challenging tasks there is in reinsurance. Questions of aggregation are entirely fact specific. In addition, they are ultimately a question of intuition and commonsense and it is this last point that

perhaps best explains why there are so many, apparently, conflicting decisions arising out of broadly the same set of facts and the same wording. A very good example of this are the many claims that emanated from the World Trade Centre attacks. As is well known in the reinsurance market some arbitration tribunals have held that the claims can be aggregated on the basis of one event (see Simmonds v Gammell [2016] EWHC 2515 (Comm)). Others have found that the claims can be aggregated as two events (see Aioi Nissay Dowa Insurance Company Ltd v Heraldglen Ltd [2013] EWHC 154 (Comm)).

Application to a Hypothetical Cyber Incident

With the caveat that aggregation is entirely fact specific, it is now worth looking at how event based aggregation may work with respect to a major cyber incident. It goes without saying there are many different types of cyber incident. However, for the purposes of illustrating the potential difficulties it is perhaps worth looking at a hypothetical global cyber attack such as the Wannacry attack in May 2017.

What happened with the Wannacry ransomware incident is fairly well known. Once a computer was infected the files were encrypted and then a ransom demand was made. Unless the user paid the ransom demand the threat was that the files on the computer would be deleted. It was reported that some 400,000 computers were infected in 150 countries and that it affected organisations as diverse as the NHS in the UK, Telefonica in Spain and Fedex in the USA. Fortunately, the Wannacry incident did not have a significant impact on the insurance industry, largely due to the fact that very few ransoms had been paid (estimated to be circa USD150,000 in total) before the kill switch for the virus was accidently discovered. However, subsequent attacks such as Petya and NotPetya have been more significant. What all of the attacks have in common is that they spread incredibly quickly across the globe, they are self perpetuating (in that they are capable of spreading by themselves across the networks), and have the potential to continue for quite some time. They do not take place at a particular time and they do not affect all insureds at the same time. One organisation can be compromised in one part of the World and then another can be compromised quite some time later on the opposite side of the World.

If one tries to apply the conventional, court determined, definition of an “event” to a wide ranging cyber attack then there are some obvious difficulties which arise. A cyber attack is completely unlike a conventional natural catastrophe such as an earthquake or a hurricane that the courts, generally, have no problem determining is one event. It is also unlike a terrorist attack such as the attack on

the World Trade Centre. The approach of the court and the many reinsurance tribunals that have had to consider whether the liabilities that followed the World Trade Centre attacks could be aggregated as one event, two events or more is quite illustrative of the potential difficulties cyber presents. This is because with respect to the World Trade Centre, and as referenced earlier, some tribunals have found it to be one event and some have found it to be two events. Where the tribunals have found it to be two events it has been persuasive that the two buildings were some 200 feet apart and there was some 30 minutes time difference between the two separate planes hitting the North and South towers. In other circumstances it has been persuasive that the attacks or security breaches that took place on the airlines prior to the planes being flown into the two towers took place at different airports and at different times. If these factors were sufficient to fail the unities test with respect to space and time then, being consistent, a cyber incident such as Wannacry might well do the same. It is fairly easy to think of a set of circumstances in which a particular reinsured may have picked up a variety of claims from an incident such as Wannacry and these claims may have come from original insureds from across the globe and in a variety of ways. Some may have straightforward cyber cover and others might have silent cyber cover. If the aggregation language in the reinsurance treaty was event based language would the reinsured be able to aggregate all of the losses and claims relating to Wannacry on the basis Wannacry was an event?

The answer to that question would obviously depend on the facts. As mentioned earlier, aggregation is entirely fact specific. On the one hand, and from a commonsense perspective, there is an argument all of the losses should aggregate and that a named global cyber attack, such as Wannacry, is an event. On the other hand, Wannacry was not something that happened at a particular time and at a particular place. It may not even have happened in a particular way. In addition, the various losses coming from a whole host of corporate insureds dotted all over the globe may not be said to be sufficiently closely connected. Whilst they would all arguably have the same cause, namely, the Wannacry malware, they did not occur at the same place and time. They might have occurred 1,000s of miles and many months apart. Wannacry could be viewed as simply a state of affairs that existed in cyberspace and it is not until each corporation was infected that you had an event you can point to. In the same way that the Court of Appeal has previously held that a riot that caused damage to 67 supermarkets belonging to an original insured was not an event. The Court of Appeal held that the losses (the damage to the supermarkets) had been caused by the acts of the rioters over a wide area, in Indonesia, at different locations and over two days (Mann v Lexington [2001] Lloyd's Rep IR 179).

The riot was a state of affairs and the damage to each supermarket was the relevant event or occurrence.

If such a situation was to ever be tested in the English court it might be that the court would be prepared to ignore (or flex to the extreme) the concept of what an event is and the unities test for the purposes of reaching a common sense decision that the losses should aggregate. However, equally, the decision might be that the parties are assumed to know what the court's interpretation of an event is and if they had wanted losses emanating from a named global cyber attack to aggregate then they would have changed the wording to something more appropriate. On the basis they kept the event language the losses do not aggregate.

Bearing all this in mind, it might be worth reinsurers and their clients revisiting their wordings. If it is intended that losses caused by a named global cyber attack such as Wannacry should aggregate then it should be relatively simple to add in language to confirm this. Although the interesting feature of aggregation is that whether it is in a reinsurer's interests to aggregate depends on the limits and size of the retention and then the number and severity of the underlying claims potentially being aggregated.

About Adam

Adam specializes in dispute resolution in the insurance and reinsurance sector. Adam also has experience of investor/state international arbitration and has acted in arbitrations under a number of the common institutional rules including ICSID, ICC, UNCITRAL and LCIA. Adam has higher rights of audience and his court experience includes a number of cases that have progressed to the Court of Appeal. He has significant experience of asset preservation and freezing orders. Adam's insurance experience encompasses a number of classes of business including financial institutions, professional indemnity, product liability, warranty and indemnity (W&I), cyber, and commercial general liability (CGL). His reinsurance experience is equally extensive and, in particular, includes advising clients on disputes involving some of the more unusual hybrid reinsurance/capital markets products. In addition to his contentious work, Adam regularly advises his clients on the drafting of new product offerings, reinsurance treaty wordings and binding authority agreements. Adam is qualified in England and Wales

Litigation News

6th Circuit Court Finds Coverage in Phishing Case

American Tooling Center, Inc., made a claim on their insurance policy with Travelers after falling victim to a series of fraudulent emails and wiring $800k overseas. The lower court found for Travelers, but was reversed by the 6th Circuit, who found the loss was a direct result of activity covered by the definition of computer fraud in the policy. As discussed in several examples last quarter – these cases have come out very fact- and court-specific.

On the coverage front, several decisions across the country denied coverage for what would broadly be viewed as "cyber" incidents when those claims were brought under non-cyber policies. Federal District Court in Florida decided Innovak International, Inc. v. The Hanover Ins. Co., 2017 WL 5632718 (M.D. Fl. Nov. 17, 2017), finding no coverage and no duty to defend under a CGL policy (coverage B) when a putative class action suit after the insureds software was hacked and personal information stolen. The Court found that the CGL language required that the insured be the party to disseminate the material, while in the situation at hand that hackers had done so. In Posco Daewoo America Corp. v. Allnex USA, Inc., et al., 2017 WL 4922014 (D.N.J. Oct. 31, 2017) Federal District Court in New Jersey found no coverage for the insured under a crime policy – the insureds customer was induced to wire money intended for the insured to the account of the hacker through social engineering. However, although the policy covered "Computer Fraud," it only covered losses involving the insureds computers. Since the hacker bypassed the insureds system entirely, there was no coverage.

Supermarket Found Vicariously Liable for Actions of Rogue Employee

Supermarket chain Morrisons' has been found vicariously liable by the English High Court for the acts of a senior IT internal auditor who released the personal details of 99,998 fellow employees of the company. The data was posted on a file sharing website and sent to three newspapers. The personal data included names, addresses, gender, dates of birth, phone numbers, national insurance numbers, bank sort codes and account numbers. The employee was convicted of offences under the Computer Misuse Act 1990 and the Data Protection Act 1998 (DPA). He was sentenced to 8 years imprisonment in 2014.

Over five thousand employees brought claims for breach of statutory duty under the DPA and at common law for the tort of misuse of private information and breach of confidence. The court concluded that whilst the DPA did not impose primary liability upon Morrisons', the supermarket chain was secondary (vicariously) liable for the actions of its employee. The judge granted Morrisons' leave to appeal. This was a liability trial only with quantum to be assessed at a later date.

Google – Snooping Through iPhones

A privacy law suit has been filed against Google in the High Court in London. In the funded litigation Google is accused of bypassing default security settings in the Safari browser to track online behavior. 5.4 million UK users are said to be affected. Google argued that these allegations are nothing new and that has defended similar cases in the past. Google paid $22.5m to the US Federal Trade Commission for the same issue in 2012.

Google Faces Possible Legal Action in the Middle East

Google's admission that it tracks phones around the world even when location settings are turned off could lead to legal action under the Cybercrime laws of Saudi Arabia and the United Arab Emirates. Android phones using Google's mobile operating system have been recording the locations of mobile masts and sending data back to Google.

TransRe Speaks

Kara Owens
will be speaking:

- **February 6th**
  IRUA “The Emerging World of Cyber Risk Insurance” – New York, NY

- **February 23rd**
  “NetDiligence Toronto “Beyond Third Party Exposure”

- **February 27th**
  AIR Cyber-Casualty Seminar

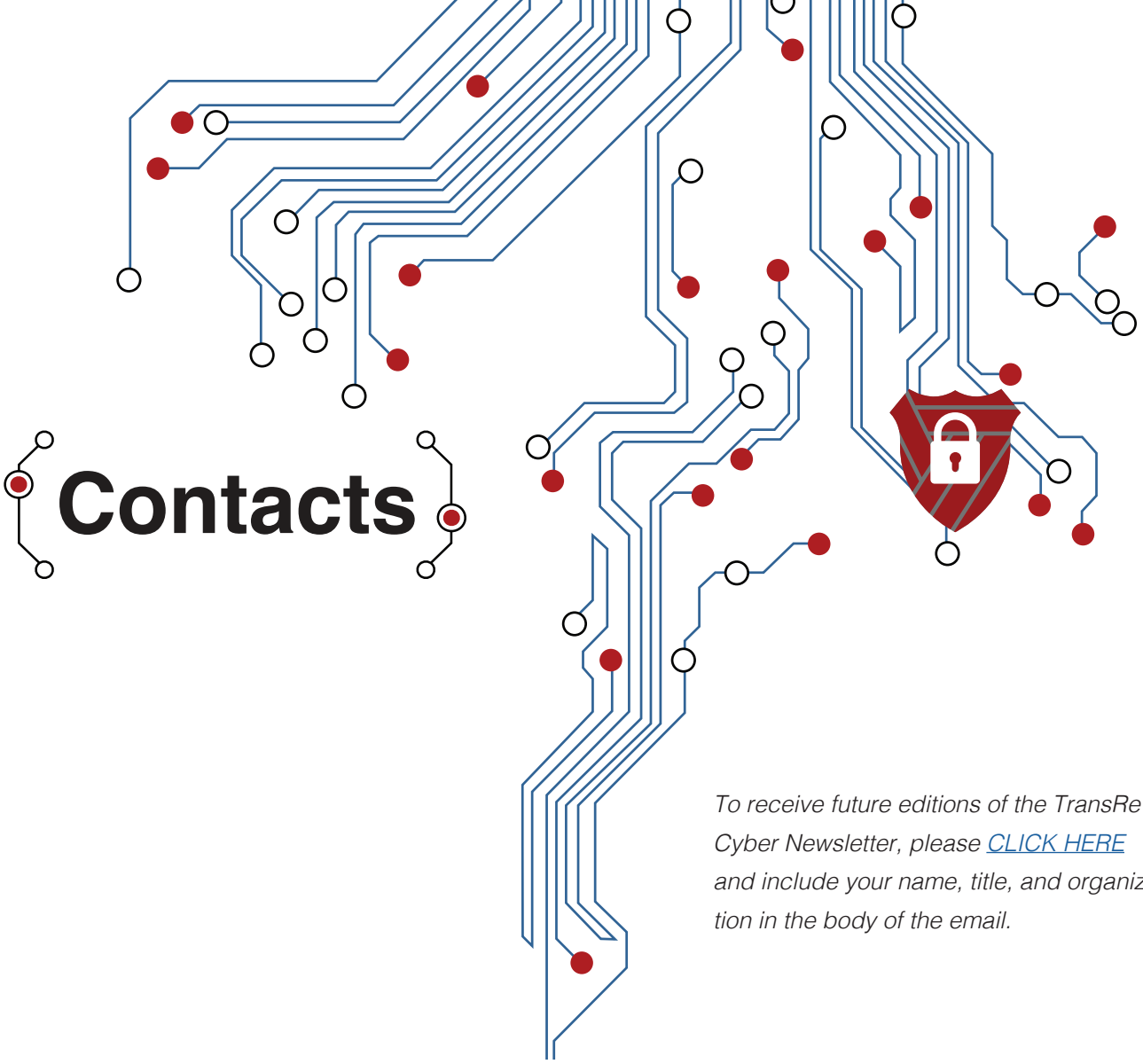
Peter Cridland
will be speaking:

- **March 21st**
  PLUS Healthcare and Medical PL “Healthcare Interlude: Swimming Upstream” (including discussion of cyber liability in healthcare)

April 8-10
Crittenden Medical Insurance Conference, “Cyber World: Data Breaches, Invasion of Privacy, and Social Media in Healthcare – Are You Prepared?”

Cyber Studies & Trends

- NetDiligence Cyber Risk News Alert – 11.30.2017
- McAfee Labs 2018 Threats Predictions Report
- PandaLabs 2018 Cybersecurity Predictions
- Information Security Forum 2018 Forecast
- Ponemon / Accenture 2017 Cost of Cyber Crime Study
- OECD – Enhancing the Role of Insurance in Cyber Risk Management



Contacts

To receive future editions of the TransRe Cyber Newsletter, please CLICK HERE and include your name, title, and organization in the body of the email.

Kara Owens
Global Head of Cyber Risk
1.212.365.2340
kowens@transre.com

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

Peter Cridland
Assistant Vice President
1.212.365.2032
Pcridland@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

Alex Bustillo
Cyber Risk Underwriter
1.212.365.2379
abustillo@transre.com

Miguel Canals
Cyber Risk Underwriter
1.212.365.2266
mcanals@transre.com

Phylip Jones
Global Marketing Manager
pjones@transre.com
212.365.2281