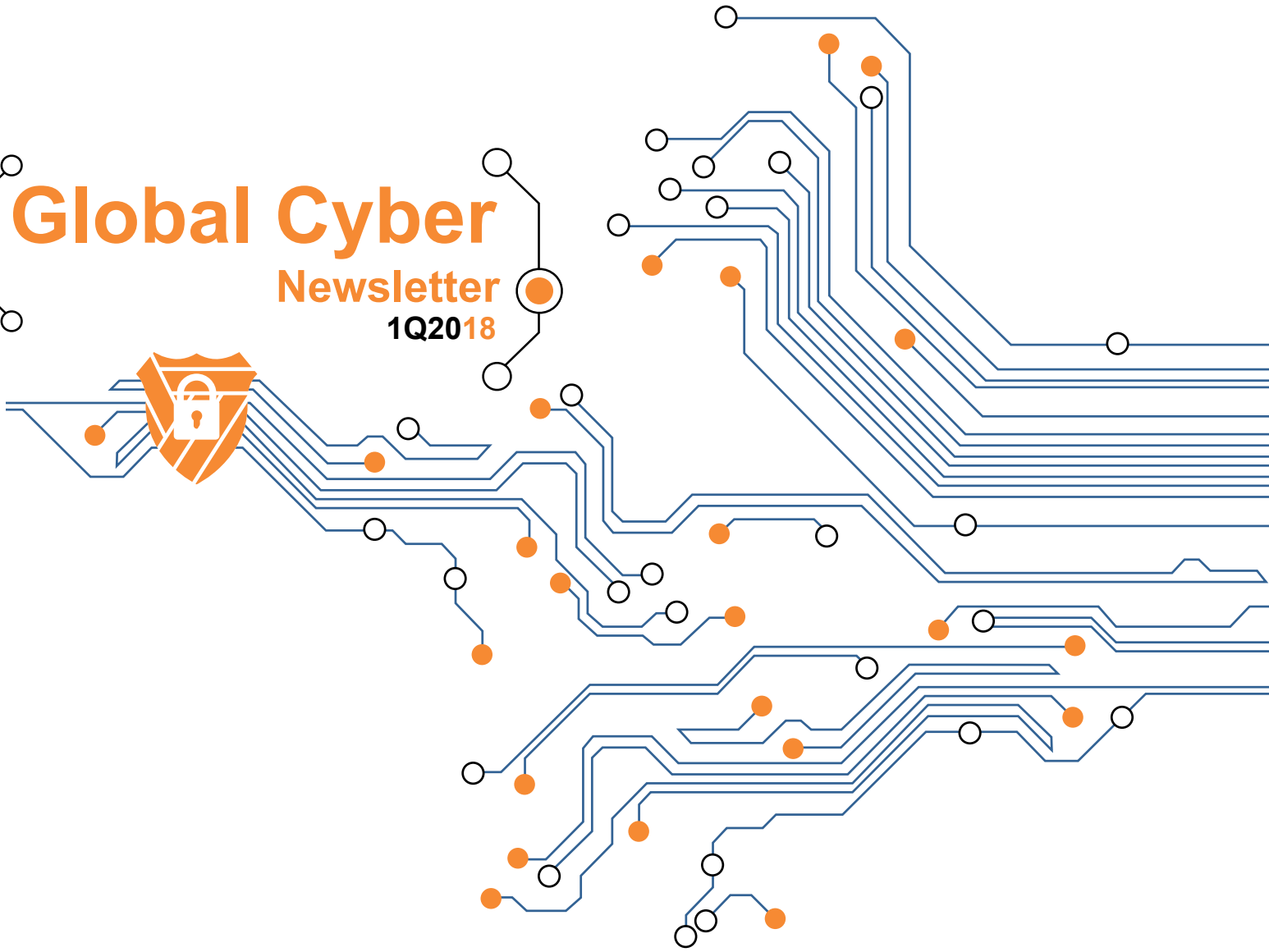
TransRe
We value risk.

Global Cyber
Newsletter
1Q2018



TransRe cyber
We value risk.

Table of Contents

Notable Cyber Breaches & Threats

Major Hardware Vulnerabilities Identified in all Devices with Intel, AMD, ARM Processors

In early 2018 one of the biggest and farthest-reaching security incidents to date was revealed: dubbed Meltdown and Spectre, these exploits make use of "speculative execution" processes in the kernel memory to access extremely sensitive data that theoretically could be used to entirely hijack the device. Since the flaw is in the processor itself, both Mac and PC's are equally affected, and it has proven difficult to patch without significantly impacting processor performance.

Although news of these flaws publicly broke in early January, they were first discovered and disclosed to the manufacturers on June 1, 2017. Even after it was publicly revealed, there were significant issues with the patches intended to remedy the vulnerability. The situation continues to unfold, with much discussion and concern focusing on the fact that Intel and the other manufacturers failed to disclose the issue to either the government or to the public, and continued to market and sell the flawed chips (and devices with those chips installed) for nearly 6 months. Intel now faces at least 32 class action lawsuits as a result. Apple and AMD also face lawsuits related to the vulnerabilities.

U.S. Enforcement: Wall of Shame Watch

The 2018 high-water-mark on the infamous Wall of Shame was set early on so far: Oklahoma State University Center for Health Sciences reported a breach involving 279,865 records on January 5th, after a third party gained access to folders containing the sensitive information. The second-largest breach reported to date in 2018 is the St. Peter's Surgery & Endoscopy Center breach involving 134,512 affected individuals after an unauthorized 3rd party gained access to its servers.

U.S. Enforcement: Federal HIPAA enforcement

The Dept. of Health & Human Services, Office of Civil Rights started 2018 enforcement actions out with a bang, leveraging a $3.5M settlement against Fresenius Medical Care North America (FMCNA) for 5 separate breaches all reported simultaneously in early 2013 for 5 different FMCNA locations. Second up, Filefax, Inc. agreed to pay $100k in settlement monies from its receivership estate after it was found to have left records of 2,150 patients vulnerable. Both agreements contained requirements for additional corrective action.

VTech Fined in Second Brush with Regulators

VTech Electronics agreed to a $650k settlement following charges that it collected digital data on children without parents' permission and then failed to keep that information secure. The company manufactures electronic children's toys and apps, and managed to collect text messages, photos, and audio messages without notifying users. VTech was previously in the news in 2015 after its servers were hacked and children's personal information was compromised.

Personal Data of 247,000 U.S. Department of Homeland Security Employees Exposed

The U.S. Department of Homeland Security revealed in January that an unauthorized copy of the investigative case management system was found in the possession of a former employee, exposing the personal information of over a quarter of a million current and former employees. According to their statement, that information did not "stem from a cyberattack" and was not exposed to "malicious activity."

Allscripts and Hancock Health: SamSam Strikes Again

In January both Hancock Health and Allscripts were infected with the same SamSam ransomware that first made its rounds in 2016. It took barely a week for Allscripts to be hit with a class action lawsuit based on the breach, and on the fact that the company had failed to secure their systems against a well-known vulnerability.

Winter Olympics

Organisers have confirmed that the Winter Olympics were hit by a cyber-attack during the opening ceremony in Pyeongchang, South Korea. The attack targeted the official website preventing access to information and the printing of tickets for events.

University Breach In Japan

An overseas hacker used the user name and password of a lecturer to access the personal data of approximately 80,000 students, graduates, staff and former workers of Osaka University on multiple occasions. Identification numbers, names and e-mail addresses are said to be in the data exposed by the breach.

Websites Hit By Cryptocurrency Mining Malware

Staying with cryptocurrencies, a common plug-in known as Browsealoud, used by websites to assist blind and partially sighted people to access the web, was infected by a malicious code. The code known as Coinhive, uses the processing power of the user's device to run processor intensive mining of the cryptocurrency Monero. Thousands of sites were allegedly affected across the UK including the NHS and Information Commissioner's Office (ICO).

Fitness Tracker Lights Up Military Bases

The use of fitness tracking devices by military personnel has been called into question. Military users of Strava fitness devices have inadvertently published their locations online. Global heat maps provided aggregated and anonymized data of billions of activities uploaded to the company's platform. The website allows users to drill down and obtain the full names of members.

Swisscom Breach

Swiss telecoms operator, Swisscom confirmed that its data systems were breached late last year with 800,000 customer contact details compromised including names, addresses, telephone numbers, dates of birth. No password or payment data was taken. Data is said to have been accessed using a sales partner's credentials.

The City of Atlanta Hit with Ransomware Attack

Atlanta is fighting an ongoing ransomware attack, with some systems remaining down over a week after the attack was initiated. There is no evidence to date that the attack has compromised personal data of residents, but the cities bill-payment system and court system are included in the breached areas. The attackers demanded $51,000 USD in ransom, and the city has not decided whether they may eventually pay it yet.

Regulatory & Legislative Update

Federal Breach Notification Legislation in the Pipeline

Several members of the U.S. House of Representatives, Financial Services Committee have made statements indicating that federal data breach legislation is likely in 2018. Hearings are underway, although the parameters of any future legislation appear far from clear.

SEC Offers New Guidance on Cybersecurity

The U.S. Securities and Exchange Commission has issued its first guidance related to cybersecurity in nearly seven years. The guidance itself in large part only reminds regulated entities of the existing framework, and does not detail significant new responsibilities. This fact was highlighted in a separate press release by Commissioner Stein, who would have pushed the new guidance farther. Notably, she indicates the possibility of requiring an 8-K notice to investors by any public company that suffers a cyber security incident.

European Commission Releases GDPR Guidance

As the countdown to application of the GDPR approaches, the European Commission recently released additional guidance for the final stages of preparation. The guidance offers additional explanation and education on what exactly is expected of the various regulated entities under the new law, and provides resources for complying with it.

Cyber Security Bill Introduced in Singapore

Following a public consultation the Cyber Security Bill which is aimed at the protection of Critical Information Infrastructure (CII) was passed by the Singapore parliament on the 5th February.

New Australian mandatory data breach notification obligations

The Privacy Amendment (Notifiable Data Breach) Act 2016, scheduled to take effect in February, will introduce mandatory data breach notification provisions for agencies and organisations regulated by the Privacy Act 1988 (PA). The legislation will require these organisations to notify the Australian Information Commissioner if a reasonable person would conclude that affected individuals are likely (more probable than not) to be at risk of serious harm as a result of unauthorized access or unauthorized disclosure of personal information. Serious harm includes serious physical, psychological, emotional, economic

and financial harm. Penalties for failure to report such a breach could be up to A$360,000 for individuals and up to A$1.8 million for organisations with an annual turnover of A$3 million.

Carphone Warehouse fined by UK regulator

The Information Commissioner's Office (ICO) has fined Carphone Warehouse £400,000 for a data breach which occurred in July/August 2015. The ICO cited a number of deficiencies in the technical provisions and security measures in place in its system including considerably out of date software. The breach exposed the data of well over three million customers and employees. Using valid login credentials, the attacker accessed names, dates of birth, marital status, current and previous addresses as well as certain details of 18 thousand historical transactions for a period between 2010 and 2011 for which cardholder names, addresses and card expiry dates were compromised.
The fine is on a par with the penalty issued to Talk Talk in October 2016.

UK loss adjusting firm fined

The ICO has fined a loss adjusting firm, Woodgate and Clark Ltd; two senior employees and two private investigators a total of £150,000 for a practice known as "blue chip hacking". Private investigators unlawfully obtained financial information, including details of banking transactions and disclosed it to an insurer investigating a fire at a business premises.

FTC Releases Annual Privacy and Data Security Update

The U.S. Federal Trade Commission released its annual report detailing the work the Commission did in 2017 to protect American consumers through enforcement actions and other means. The Commission undertook over 130 spam and spyware cases and 50 privacy lawsuits, including against computer manufacturer Lenovo, ride-sharing company Uber, and networking equipment manufacturer D-Link, amongst others.

Global Cyber Security

Cybersecurity a Top Concern for U.K. SMEs

According to Barclays Business Banking's annual SME Hopes and Fears Index, Cyberattacks are the #2 concern for 2018. This ranks the issue behind inflation, but ahead of the "state of the UK economy" – notable in the Brexit era. The report also indexes hopes for 2018, with "availability of better technology" and "E-commerce / digital presence" taking the 2nd and 3rd spots on the list.

Malicious Security Apps Found in Google Play

At least 336 apps were found in the Google Play store that harvest data on users and push advertisements to them. These malicious applications were discovered by the cyber firm Trend Micro in January, and it is unknown how many users downloaded the apps before they were pulled.

Smart Home Cryptojacking Worries Increase with Price of Bitcoin

The value of Bitcoin soared in late 2017 and early 2018 was mirrored by a rise in incidents of cryptojacking, in which victim's devices are hijacked to mine cryptocurrencies for other people. However, targets have not been limited to large-scale computers; at-home internet-connected devices from thermostats to lightbulbs have been targeted in the same manner. Many of these devices lack the basic security to protect them, much in the same way that botnet attacks have previously made use of the aggregate power of large numbers of low-power devices.

Long-Term Hack by Lebanese Government Uncovered

Researches from the Electronic Frontier Foundation and cybersecurity company Lookout recently released a report detailing a malware campaign going back to at least 2012, and linked directly to a specific building in Beirut owned by the Lebanese inteliligence agency, the General Security Directorate. The effort appears to use spearphishing and fake login pages, and captures passwords, photos, and location data, amongst other details. Of particular note, the hacking effort made use of servers previously linked to a hack by the government of Kazakhstan – one of several indications that the servers and perhaps the malware itself is being rented out by a third party to different nation-states.

Factory Safety Systems Compromised by Cyber Attack

Hackers successfully infiltrated the safety systems at a petrochemical plant in Saudi Arabia, in an attack similar to the infamous Stuxnet. Although many details were difficult to confirm, the manufacturer of the safety device at issue did confirm that the device had been compromised and could have functioned as though everything was normal even as damage was being done to the facility. No damage was done in this instance – more likely the breach was a "proof of concept." The same safety system is widely used at nuclear power plants and oil and gas facilities, raising the spectre of large-scale physical damage originating from a cyber attack.

Facebook Data Scandal

Social media giant Facebook faces allegations that it worked with data analytics firm Cambridge Analytics to mine detailed personal information about at least 50 million Facebook users and use that data, in one instance to help the Trump campaign reach the White House. Many of the allegations came to light after a journalist went undercover and filmed Cambridge Analytics CEO Alexander Nix providing examples of how they could help construct a smear campaign against political rivals. The repercussions have been swift: Facebook's Mark Zuckerburg has been summoned to appear before both the U.S. Congress and the U.K. parliament, and Facebook book value has taken a $60 billion hit since the scandal broke.

Largest Cryptocurrency Theft to Date Hits Coincheck

Japanese cryptocurrency exchange Coincheck was breached, with hackers stealing about $530M USD in the cryptocurrency NEM. That number tops the infamous Mt. Gox theft of 2014 in which roughly $450M USD was stolen. At least 260,000 Coincheck customers were affected, with Coincheck promising to reimburse customers out of their own capital – although customers have begun suing the exchange when that reimbursement has not been forthcoming. The hackers responsible have already begun trying to sell the stolen currency with unclear success.

More Cryptocurrency news…

Inevitably, the world of cryptocurrency endured several significant shifts this quarter in addition to the items noted above.

• Research revealed the vulnerability and volatility of cryptocurrency pricing by showing how one person likely caused the entire market to plunge in a single day.

• Cryptojacking has entered the mainstream lexicon – particularly after it was revealed that thousands of U.K. government websites were hijacked, including the ICO.

• Bitcoin continues to lose utility as a currency: Lloyds will now block Bitcoin purchases on its credit cards, and ironically, a major Bitcoin conference in the world will no longer accept Bitcoin in ticket purchases.

• The SEC has issued subpoenas targeting tech companies, individuals, and others involved in Initial Coin Offerings (ICOs), suggesting a crackdown is in the works. ICOs mimic the more well-known (and well-regulated) IPOs in name and intent, but SEC Chairman Jay Clayton has stated that zero ICOs had registered with the Commission as of February 6th. The SEC also issued a statement asserting that cryptocurrency trading platforms should register as security exchanges.

• Similarly, the Commodity Futures Trading Commission charged one small cryptocurrency trading advice firm with fraud, and a recent court ruling held that cryptocurrencies fall under the Commodity Exchange Act, providing the CFTC with firmer standing to pursue additional, larger enforcement actions.

• Ethereum - still the second-largest cryptocurrency after Bitcoin by a large margin – recently faced news that a vulnerability in the system could allow ether to be double-spent, striking a blow to the primary function of the blockchain technology on which cryptocurrency is based.

Guest Article

Data Protection and Mandatory Breach Notification: Developments in Asia

By Bryan Tan, Partner Pinsent Masons

Overview

Looking out from Asia, data protection law generally lags behind that of Europe. Europe is generally regarded as the gold standard in data protection and even more so with the impending arrival of the GDPR. However, this gap is closing fast and the relative position of Asia data protection law vis-à-vis European data protection law has narrowed much in the last 10 years. China and the Philippines have recently taken steps towards the enactment of comprehensive data protection legislation. Japan and Australia have recently made amendments to their existing data protection laws - hardening enforcement and introducing mandatory breach of notification requirements respectively. Thailand and Indonesia are taking steps towards the introduction of data protection legislation, while Singapore and Hong Kong are reviewing their legislation. In addition, the APEC Cross-Border Privacy Rules system which has been enacted since 2011 has recently been boosted by announcements that several Asian countries including Korea, Singapore, Philippines, Australia, Hong Kong, Taiwan and Vietnam are considering joining it. Thus, the case can be made that Asian jurisdictions are making up ground on the development of their data protection frameworks.

Mandatory Breach Notifications

An important marker in the maturity of a data protection system would be its breach notification requirements. In Asia currently, South Korea, Indonesia, Philippines and Australia do not have mandatory breach notification requirements. China, Hong Kong, Singapore and Japan do have sector based mandatory notification requirements while Hong Kong and Singapore have voluntary breach notification regimes for non-sector breaches. Indeed countries like Singapore and Australia are now seriously considering proposals to introduce mandatory breach notification, not unlike those of the GDPR. Also, following a series of wide spread data breaches, calls have been made for Malaysia to introduce mandatory breach notification requirements. The trend is clear – slowly but surely mandatory breach notification requirements will be introduced in data protection laws in Asia.

A note has to be added about the resistance to mandatory breach notification by organizations that collect personal data. Mandatory breach notification requirements, they argue, are an onerous burden on organizations and at times, impede investigations into cyber security incidents. A mandatory breach notification would also inadvertently tip-off the perpetrators and defeat any attempts to apprehend them. However, the public outcry over organizations keeping silent for inordinate periods of time or even worst feigning ignorance, has led to calls to implement mandatory breach notification requirements similar to that of more advanced economies.

Requirements for Mandatory Breach Notifications

Therefore, the question now is if an Asian country were to impose mandatory breach notification requirements, what would some of those requirements look like? I would suggest the following:

1. Response time - there must be a reasonable response time given to organizations to respond or to make the mandatory breach notification but the clock cannot tick on indefinitely. There must also be efforts to notify the affected the individuals in order for them to take self-help steps to protect themselves. Typically, a 72 hour response time has been mooted. Of course, if circumstances were such that a mandatory breach notification would cause more harm than good, for instance, where a cyber intruder is still lurking in the system but has not yet undertaken damaging action, a longer response time while efforts to track and trace the intruder takes place might be viewed as reasonable.

2. Who to notify – surely the effected individuals would be on such a list but in addition, consider which regulatory authorities should receive such notifications. Should this be just the data protection commissioner or should it include the full range of regulators including sector regulators and law enforcement? While more is generally good, the expansion of resources in a time-critical period to satisfy duplicate notification requirements may not be a wise move.

3. Severity – what level of severity would trigger the mandatory breach notification and if so, to which group of persons? Would a breach involving non-sensitive data of a small group of individuals be sufficient to trigger the requirements? How massive must the breach be to justify a notification and

how sensitive must the data involved be? On one hand there might be some utility in a centralized information collector who may be able to identify trends from small data breaches reported by large number of organizations but on the other hand too low a severity level might result in onerous requirements on organizations and overwhelming amounts of data being received.

4. Format and content of notices – how should such notices be received and what information is required in such notices? Are data organizations required to provide their remedial plans, forensic analysis and are they required to offer compensation and other tools to the affected individuals?

5. Penalties –should penalties be imposed on the failure to notify a breach? Conversely, should incentives be given to organizations that report a breach perhaps with a stay of regulatory enforcement while investigations are ongoing after a breach is reported.

6. Harmonization – would it be beneficial if countries take a similar approach to mandatory breach notification? As a simple example, different response time requirements will lead to a less than ideal situation where one regulator gets information before the other regulator in a neighboring country. Given that Asian economies are increasingly interconnected, a case can also be made of harmonization of some portions of data protection law which cut across national boundaries. Mandatory breach notification is one such possible area.

Be that as it may, the trend of regulatory breach notification admits an increasing incidents of wide spread data breaches, mandatory breach notification will soon reach the shores of Asian jurisdictions. In fashioning these requirements, regulators will undoubtedly face these issues and have to address them. We await these developments with bated breath.

Qualified in both England & Wales and Singapore, Bryan practices in such areas as finance, information technology, telecommunications, biotechnology and bioinformatics, Chinese intellectual property, entertainment law, and corporate work. He advises corporates, institutions as well as governments. He has given numerous talks in Singapore and abroad to research institutes, universities, governments, and industry bodies. He is an author of Halsbury's Laws of Singapore - E-Commerce and Halsbury's Laws of Malaysia - E-Commerce (both editions). He also co-wrote the Singapore chapter of "Electronic Evidence" and the Singapore chapter of "Higher Education". Bryan also has a regular column on ZDNet on legal tech issues.

Litigation News

AIG Subsidiary Asserts No Duty to Defend Yahoo in Email-Scanning Suits

Yahoo resolved the several class action lawsuits concerning its practice of scanning emails to and from "@yahoo.com" email addresses in 2016. However, the lawsuit between Yahoo and its insurer – AIG subsidiary National Union Fire Insurance Company of Pittsburgh, Pa – as to whether the insurer had a duty to defend Yahoo under their CGL policy against such broad claims continues. AIG has filed a motion for summary judgement that is now pending in the Northern District of California.

Zappos Class Action Lawsuit Reinstated

A class-action lawsuit based on the 2012 Zappos data breach that exposed information on more than 24 million consumers has been revived by the 9th Circuit In a recent ruling, that court found that the risk of identity theft resulting from the breach was "imminent", and that was enough to establish standing for consumers whose information was exposed but have not yet become victims of identity theft.

U.S. Supreme Court to Decide Impact of International Borders on Data

The case U.S. v. Microsoft is currently before the Supreme Court, the issue being whether U.S. corporations are required to turn data stored on overseas servers over to U.S. law enforcement in response to a search warrant. With a ruling expected later in the year, the case could have broad implications in the near term, but could also push Congress to pass legislation settling the issue – one such proposal is currently pending in the Senate, and has the support of several tech companies, including Microsoft.

TransRe Speaks

Miguel Canals

will be speaking:

- **June 11th-June 14th**
  2018 Miami Latin America Claims (Re)Insurance Forum - Miami, Florida

Peter Cridland

will be speaking:

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

Cyber Studies & Reports

- Thales Data Threat Report
- Troutman Sanders - Data Privacy: The Current Legal Landscape
- Aon 2018 Cybersecurity Predictions
- Crowell & Moring Regulatory Forecast 2018
- ID Experts Data Breach Examiner
- NetDiligence Cyber Risk News Alert

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.

Elizabeth Geary
Global Head of Cyber Risk
1.212.365.2243
egeary@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
1.212.365.2376
abustillo@transre.com

Miguel Canals
Cyber Risk Underwriter
1.212.365.2266
mcanals@transre.com

Phylip Jones
Global Marketing Manager
1.212.365.2281
pjones@transre.com