TransRe
We value risk.

Global Cyber

Newsletter

3Q2018

TransRe
We value cyber 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.

TransRe
We value risk.

Welcome to our cyber newsletter.

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

“What’s past is prologue”
William Shakespeare

With each client, broker and vendor meeting I am reminded that the term ‘cyber’ has breadth in definition, which can lead to confusion. Cyber impacts all lines of business, both as a hazard and as a specific coverage / product. As an industry we must understand the different exposures in our stand-alone portfolios, as well as cyber in other lines of business. With the increased reliance on technology and the speed at which new vulnerabilities or threats emerge, underwriters must keep informed and continue to assess cyber risk as it evolves. We need to be proactive instead of waiting for loss patterns to emerge and then react – a history with which we as an industry are quite familiar. For underwriters the past is prologue, and the future is now.

As cyber affects all lines of business, it is important to distinguish between ‘cyber’ - the all-encompassing threat/hazard to every digital business and ‘Cyber’ - the line of business / product.

So what do we mean by cyber as a hazard….? All companies use computers and other devices connected to the internet to conduct everyday business. Malicious or accidental cyber incidents can result in losses from otherwise covered perils, such as a hack causing a fire. Traditional insured risk has changed – new technology, its interconnectivity and our increasing dependence on it have converged to change every risk profile.

Here are a few real and hypothetical examples of cyber as a hazard leading to covered perils in some traditional lines of business:

Commercial Property: A German steel mill has its control system hacked which causes a fire leading to millions of dollars in property loss. (2015) First party: physical damage and business interruption. Cyber as a hazard; fire as a peril.

Homeowners: A burglar buys a homeowner’s credentials on the dark web and pins his way in to the “smart” home. First party: theft. Cyber as a hazard; theft as a peril.

Directors and Officers: Yahoo! data breach (2013) finds the directors and officers liable for failing to encrypt its users’ personal information. Potential: Side C Entity Coverage; Side A Derivative Coverage. Cyber as a hazard; D&O failure as a peril.

Marine: Hackers take control and steer one ship in to another. Hull: physical damage; P&I: bodily injury. Cyber as a hazard; collision as a peril.

Cyber as a hazard requires an adjustment in underwriting approach (including policy wording); all underwriters will have to become part-time cyber underwriters as the risk landscape continues to change.

The above examples of a cyber hazard triggering traditionally covered perils needs to be distinguished from where Cyber itself is the insured peril or coverage. When Cyber is written specifically – on a stand-alone basis, or as part of a policy or endorsement – coverages may include first party (data breach response, cyber extortion, data recovery, and business interruption) and third party (network security liability, privacy liability, and some regulatory costs).

Specific cyber coverage necessitates a combined underwriting / IT specialist approach with evaluations of: how exposed or vulnerable is the company from a security standpoint? What back-up plans are in place? How is personally identifiable information or other data protected? What is the patching cadence and effectiveness? In addition to the risk assessment, what coverages are provided? If writing excess-layered

business, is the intent of coverage aligned with the primary forms? Cyber underwriting requires a special strategy for assessing, pricing and aggregating the risk. If Cyber coverage is offered across various lines of business, it needs to be underwritten with the same diligence as stand-alone Cyber, and aggregated centrally within the company.

One recent example in the market that highlights the need for a cohesive strategy and communication across departments within companies is the NotPetya loss, where the property form for a number of impacted companies is believed to include affirmative coverage for non-physical cyber damage, and ensuing business interruption at much larger limits than the cyber tower. The resulting loss from lines of business outside of stand-alone Cyber may in fact actually drive the majority of the over $3B NotPetya industry loss. When Cyber is offered in other lines of business, we must pay especially close attention to systemic risk potential – such as business interruption and contingent business interruption.

Identifying and properly assessing the changes in risk exposure due to cyber both as a hazard and as a peril / coverage is the work of a full team – education of all underwriters; reviewing the policy wording for every line of business – primary and excess; addressing the intent of coverage; reassessing the effectiveness of exclusions; ensuring corporate buyers have gapless, transparent protection (no silent policies); working with the cyber team to properly assess the dynamic risk threat; having a feedback loop with claims and actuarial to inform and refine the risk assessment; and managing risk aggregation across all lines of business.

The past is prologue. What happens next is the crucial act(ion). We're not paranoid, but we must be vigilant and stay ahead of the risk curve.

Elizabeth Geary
Global Head of Cyber

Table of Contents

Notable Cyber Breaches & Threats

Uber Agrees to Record $148M Fine Over 2016 Breach

Uber and the Attorneys General for all 50 U.S. States and the District of Columbia have reached a settlement over the 2016 data breach affecting 57 million riders that Uber covered up for nearly a year – as reported in the 4Q2017 TransRe Cyber Newsletter. Uber has now agreed to pay a $148M USD fine as well as take steps to address data security.

Chinese hotel chain investigates huge breach involving 500 million records

Investigations are underway in China into how the records of millions of customers of Huazhu group were compromised in a data breach. 500 million customer records of the hotel chain which operates nearly 4,000 hotels are said to have been breached with 150 million for sale on the dark web. Reports suggest that issues within the Wi-Fi management and certification system allowed hackers to access names, ID numbers and other personal information. Huazhu Hotels Group, LTD., is a publically-traded company listed on NASDAQ and has lost nearly 20% of its value since the breach was made public.

More data woes for Facebook

Facebook has revealed that the data of 50 million of its users was exposed in a recently discovered data breach. Hackers are understood to have exploited a vulnerability in its 'View As' feature. There has been no confirmation as to whether any data had been misused. The company's share price dropped 3% following of this latest data breach. The breach will be unwelcome news to the Facebook which follows the ongoing investigation into its role in the Cambridge Analytica scandal.

Singapore breaches to be investigated by regulator

The personal details of 1.5 million patients of SingHealth, including those of Prime Minister Lee Hsien Loong, were accessed & copied in a major data breach. The patients of Singapore's largest group of healthcare institutions visited the clinics between May 2015 & July 2018. A front-end work station is believed to have been infected by malware. Names, addresses, gender, dates of birth and NRIC numbers were stolen by the perpetrators.

Separately, it has only recently been discovered that 70,000 member investors of the Securities Investors Association Singapore (SIAS) had their personal details accessed illegally in 2013. Vulnerabilities in the SIAS website were exploited in the attack accessing names, NRIC numbers and telephone numbers.

Major Thai banks targeted in data heist

Two commercial banks in Thailand have suffered recent data breaches. Personal details were leaked of 120,000 customers who had applied for credit at Krung Thai Bank were compromised in addition to the data of 3,000 corporate customers of Kasikornbank using its online bank guarantee service. It is not known what type of data was accessed. Neither bank has identified any suspicious transactions.

Breach halts iPhone chip production

The world's largest contract chip manufacturer has had production disrupted by a computer virus. Taiwan Semiconductor Manufacturing Company (TSMC) is the sole manufacturer of the main processor in the Apple iPhone. The virus, which is not thought to have been introduced by a hacker, is said to have hit a number of its fabrication tools. Impact was expected to be limited as the manufacturer is said to be prepared for such disruptions.

Airline data breaches

Personal and financial details of 380,000 customers who used British Airways website or mobile app has been stolen. Customers affected were those who made or changed bookings between 21st August and 5th September 2018. No details have been released on the nature of the attack. Bank credit card details including expiry dates and CVV codes were stolen in addition to names, billing addresses and e-mail addresses. Travel and passport details were not compromised. The Information Commissioners Office (ICO) and affected customers have been notified with BA promising compensation to those affected. There have been some reports of fraud on customer credit cards.

The mobile app of Air Canada was also compromised in August resulting in the airline having to lock all mobile app customer accounts. Of 1.7 million mobile app users only 20,000 profiles may have been accessed. In addition to names and contact details, customer profiles on the app may have included passport details.

Holiday firm breached

UK Holiday firm Butlin's, announced a data incident affecting 34,000 customers following a phishing attack. Compromised data included lead guest names, postal, e-mail addresses, telephone numbers, booking references and the holiday arrival dates. The ICO has been notified. No payment details were compromised.

Dixons Carphone revises breach estimate

Technology retailer, Dixons Carphone has revised its estimate of the number of records compromised during its 2017 data breach to 10 million. The company has also now confirmed some of the data may have left its systems.

Snail mail mix-up

The personal details of customers have been included in letters sent to other customers of energy giant NPower. 5,000 customers are believed to have been affected. The ICO has been informed.

Patient management system vulnerabilities fixed

Vulnerabilities in a practice management system known as OpenEMR potentially put 100 million patient's data at risk from hackers. The system used by many surgeries and hospitals globally is used to manage information and the treatment of patients. Many of the bugs are believed to have now been patched.

Family Orbit Exposed 281 GB of Children's Photos

Family Orbit, a company that that sells spyware to parents, left the massive trove of pictures in a database protected only by a key that was also public-facing. As noted in the source article, this is only the latest in a long string of consumer spyware breaches.

Satellite Systems Hacked

Satellite systems used by transportation services and the military have been found to contain bugs that could not only allow hackers to damage the equipment, but also to discover the exact location of deployed military forces.

LATAM Targeted by Dark Tequila

Mexico and Latin America in general have avoided being targeted by many of the recent malware attacks, but a long-running malicious program has been discovered doing just that. Dubbed Dark Tequila, it has been active for at least five years, stealing financial and other personal information primarily from Mexican users. The program is spread through a combination of spear-phishing and infected USB drives.

Regulatory & Legislative Update

GDPR complaint spike

Regulators across Europe have reported a sharp hike in complaints to regulators after GDPR.

EU to protect free and fair elections

The European Union has announced proposals to fine groups that misuse voter data to influence elections in light of the Facebook Cambridge Analytica scandal.

UK's Tesco Bank fined £16.4m by regulator for cyber attack

The Financial Conduct Authority (FCA) fined Tesco Bank for a lack of due skill, care and diligence following an attack in November 2016 which resulted in the loss of £2.26m from customer accounts and service interruption. Fraudsters exploited deficiencies in the design of its debit card and the bank's financial crime controls. The FCA considered the bank's response lacked sufficient rigour, skill and urgency to what was a 'largely unavoidable' attack. A potential fine of £30.5m was mitigated by good cooperation with the regulator, a comprehensive redress programme and early payment. No data was lost in the incident.

Equifax fined by the ICO

Credit reference agency, Equifax has been fined £500,000 by the ICO for the cyberattack between May and July 2017 that exposed the personal information of 15 million UK data subjects whose data was held in the US. The UK records were part of a total breach of 146 million records. The attack exploited a vulnerability in the Apache Struts 2 web application framework used by Equifax in its consumer facing online disputes portal. The company was alerted to the critical vulnerability in March 2017 by the US Department of Homeland Security Computer Agency Computer Emergency Readiness Team. However, the company failed to implement the patch on this particular portal. The fine imposed was the maximum available under the applicable data protection law at the time. Penalties now available under GDPR could have been far more substantial.

U.S. NIST Small Business Cybersecurity Act Becomes Law

Originally proposed in April 2017, the NIST Small Business Cybersecurity Act passed into law in August 2018. The law requires the NIST director to issue guidance and a consistent set of resources to help SMBs identify, assess, and reduce their cybersecurity risks.

Governments Continue Tech Push to Access Private Messages

A new law has been proposed in Australia that would force global tech giants like Apple, Google and Facebook to allow law enforcement to access messaging on their platforms. This goes beyond obtaining warrants; if tech companies argued they were unable to provide such access, the law would allow prosecutors to force the tech companies to write code that would allow access. This is reminiscent of Apple's 2016 fight with the U.S. Government, one that is seeing a second act in America play out between Facebook and the U.S. Department of Justice. However, it would be inaccurate to take from this that these tech giants are protecting their users privacy – Facebook CEO Marc Zuckerberg's Congressional testimony discussed last quarter is one demonstration of that, as are recent investigations into the "personal assistant" systems like Siri and Alexa that are always listening to every word said by their users.

Global Cyber Security

Majority of $3B+ USD Insured Losses from NotPetya from "Silent" Coverage

According to the Property Claims Service, total ultimate insured losses from the global NotPetya virus have topped $3B as the one-year anniversary of the attack passed in June. Silent losses – and possibly affirmative covers on standard lines – may account for more than half of that total, and a large portion of that silent exposure is thought to reside on the property side, although contract language in the potentially-effected covers and possible coverage disputes remain open questions.

Google Tracks Users Regardless of Privacy Settings

The Associated Press uncovered, and Princeton University researchers confirmed, that many Google services store location data even when the user sets a privacy setting to prevent Google from doing so. Notably, this finding specifically contradicts Google's explicit assertions found throughout the permissions and "help" pages on the subject. This privacy issue is thought to affect roughly two billion users on both iPhone and Android devices. Within a week of this discovery, a class action lawsuit was filed against Google.

FBI Warns of Global ATM Threat

In early August, the U.S. FBI issued an international warning to banks that cyber criminals were likely planning an ATM "cash out" scheme using an unlimited operation breach. The breach allows criminals to disable daily maximums and other fraud controls so they can use stolen card data to empty multiple bank accounts. Two days after that FBI warning became public, Indian bank Cosmos was breached and nearly $2M USD stolen in fraudulent bank transfers, as well as $11.5M stolen in unauthorized ATM withdrawals from ATM machines in 28 countries.

Proof of Concept for Medical Equipment Hack Shown at Def Con 26

A security researcher with McAfee showed how the signal carrying patient vitals can be manipulated between the monitoring device and the central monitoring station. The process allows the hacker to pose as the central monitoring station and capture the actual data sent from the patient monitoring equipment and then to send altered patient data to the actual central monitoring station. The ramifications are myriad: all manner of improper treatments, lack of treatments, or prescriptions could be triggered by the manipulated data.

Popular Mac OS App Sent Data to China

Adware Doctor, a popular adware-blocking app for use on Mac OS computers was found to collect the browsing history of anyone using the app and sending it to a server located in China – all without the users' permission or knowledge. This action is against Apples rules for apps, and Apple appears to have removed the app from the App Store hours after the story broke.

International Studies Show Huge Cyber Losses

Recent studies have revealed that the true cost of cyber incidents may be much higher than previously understood. One study cited over $1 trillion in global losses from cybercrime, a number they note far exceeds the record $300B in damage from natural disasters in 2017. Elsewhere, a report out of Germany alone found roughly $50B in damage to the German economy from cybercrime.

CryptoCurrency Corner:

- Bitcoin mining – the process of "spending" computer processing power to verify bits of transactions in exchange for small pieces of bitcoin – is nothing new. However, the real-world effects of that computer processing power are drawing a lot of power, and attention, to the process. It was estimated that the amount of power consumed by the bitcoin network exceeded that of the Republic of Ireland in November 2017, and the amount of CO_2 emissions expended to create that power is roughly equal to that produced by 1,000,000 transatlantic flights.

- Always-volatile BitCoin value dropped below the "psychologically significant" $7,000 mark again in early September, and has been trading in the low-to-mid $6,000 range since. Note that this remains above the ~$4,300 it was trading at one year ago, but well below its peak of roughly $20,000 in late 2017.

- Perhaps related to the wild ranging value of BitCoin, the number of lawsuits mentioning the cryptocurrency have shot up in 2018: there have been three times the number of lawsuits in the first half of 2018 as there were for the entire of 2017. The U.S. Securities and Exchange Commission is responsible for many of those cases, another signal that there will be increased regulation in the cryptocurrency arena.

- One such SEC case, Crypto Asset Management settled for a $200k fine in early September. In another case, broker-dealer TokenLot agreed to disgorge $471,000 in profits related to their sale of cryptocurrency investments, in addition to additional fines of $45k each against the two individuals who launched TokenLot.

TransRe Speaks

Elizabeth Geary

will be speaking:

- **Thursday, October 25th**

  Advisen Cyber Risk Insights Conference - New York, New York

Peter Cridland

will be speaking:

- **Friday, October 12th**

  CLM Cyber Summit - New York, New York

- **November 7th-9th**

  PLUS International Conference - San Diego, California

Litigation News

Facebook granted leave to appeal by the Irish Supreme Court

Facebook has been granted leave to appeal to the Irish Supreme Court a decision by country's High Court to refer a number of key questions directly to the Court of Justice of the European Union (CJEU). The questions arise out of the usage of 'standard contract clauses' for the transfer of data between the EU & US. The appeal focusses on a number of aspects of the lower court's decision including the validity of the referral to the CJEU; whether EU law applies to the processing of personal data for national security purposes and whether EU data subjects have an effective remedy for the 'mass indiscriminate processing of data' by US surveillance agencies.

Neiman Marcus Class Decertified

As class action litigants continue to struggle to advance through the process after cyber breaches, one of the early such class action suits has hit another stumbling block. The District Court rejected a proposed $1.6M settlement, and decertified the class.

Cyber Studies & Reports

The Office of the Australian Information Commissioner (OAIC) has issued its second report following the introduction of the Notifiable Data Breaches scheme which was introduced in February 2018. Notification obligations apply to entities where a breach is likely to result in serious harm to the individuals. 305 incidents have been reported since the scheme began. 242 notifications were made in the 2Q, 59% of which resulted from malicious or criminal attacks. 36% resulting from human error. The health service providers and finance sectors were the top industry sectors affected.

- EIOPA Understanding Cyber Insurance
- Aon Cyber Insights – Q2 Review
- Troutman Sanders Data Privacy Newsletter


Hacking the Internet of Things (IoT)

In 2015 I read an article about a security expert that managed to crack the password to the mobile phone app that was used to control a household “smart” kettle. This means if you were lucky enough to own one, he could remotely control your kettle. I remember thinking, as a man who needs a litre of coffee to function in the morning, that’s powerful stuff. What happens if he doesn’t let me turn it on? Or as a force for good, possibly he may just switch it on at 5:45am, so it’s ready for me when I emerge.

Putting those thoughts aside, it was probably only a further year or so on before we saw a more serious attack taking place on and using IoT devices. On October 12th, 2016 a large scale distributed denial of service attack took down or certainly hindered the internet traffic for the whole US Eastern seaboard.

The Dyn attack, used the Mirai malware to scan the internet for the IP addresses of IoT devices, such as printers, CCTV cameras and consumer internet routers. Mirai then identified vulnerable devices using a table of over fifty common factory default usernames and passwords and logged into them to infect them with the Mirai malware as well. IoT devices, which by nature must be easy for the consumer to install, have very little that you can configure to make them less vulnerable. In the IT security world default settings are something we seek to eradicate from our networks.

Once infected by Mirai the devices report into a command and control server, which then provides them with a target. The reason why distributed attacks are successful is that protection technology generally looks for abnormal traffic patterns, for example one IP address sending a large volume of data that it can then block, clearly something made immensely more difficult and time consuming to distinguish when you are dealing with a vast number of multiple instances. Also, with a distributed attack the bad actor can harness a lot more computing power and bandwidth than they can from their own bedroom or shed.

The Dyn attack essentially gathered the IoT devices, assembling a “botnet” or network of private, in this case mini-computers to wreak havoc on the internet. The actual attack got the botnet to simultaneously conduct thousands of Domain Name lookups, (the process of checking into a server to translate a web address to an IP address), on the servers run by the company DYN.

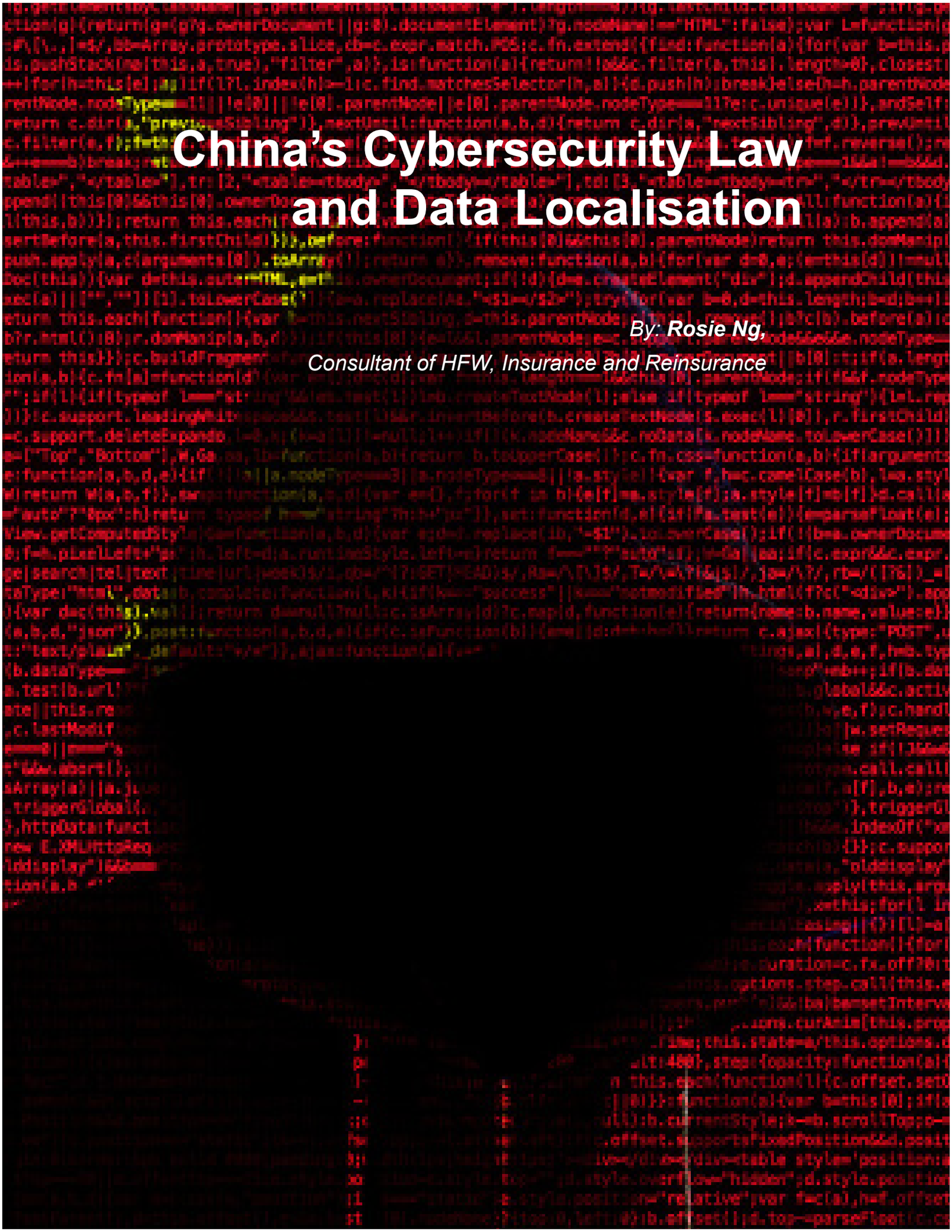
The more devices, the bigger the problem and its projected that by 2020 there could be as many as 25 billion – some security companies suggesting around a quarter of all cyber-attacks will target IoT devices. I’m sure many people reading this may now be reaching for an old-fashioned kettle they can put on their gas stove, but I think we can all agree the convenience of many devices means in today’s age that’s not
going to happen.

Neil Inskip*, VP, IT Manager Information Technology - Europe*

China's Cybersecurity Law and Data Localisation

By: ***Rosie Ng,***

Consultant of HFW, Insurance and Reinsurance



Introduction

On 1 June 2017, China's Cybersecurity Law ("CSL") came into effect. This is the first comprehensive legislation of its kind providing a framework for data protection and governance of network and system security. The CSL applies to (i) Network operators, and (ii) Critical Information Infrastructure Operators.

Network operators

"Network operators" are defined as "owners, operators and service providers of networks". "Network" is deemed to be any system comprised of computers or other information terminals or equipment which are used for the gathering, storage, transmission, exchange and processing of information.

The CSL applies not only to businesses in China which manage their own data network but also companies based outside China who use networks to conduct business there.

Critical Information Infrastructure Operators ("CIIO")

CIIO are entities which provide services which, if lost or destroyed, would seriously damage China's national security, economy or the public interest. The CSL provides examples of these, such as entities which operate in the public communications and information services, energy, transportation, water resources, finance and public services sectors.

Duties and obligations

The CSL imposes a number of key obligations on Network operators.
With regard to network systems, they are required to:

- Set up internal security and management systems and procedures, including the appointment of appropriate personnel to effect a secure network.
- Take technological measures to prevent viruses, combat cyber attacks and threats to network security (including monitoring the network activities carried out by their users).
- Keep a record of network activity and security breaches and to maintain this for a minimum of 6 months.
- Take security measures such as data classification, back-up systems and encryption.
- Set up a complaints reporting procedure.

With regard to personal data, they are required to:

- Seek and obtain consent from the relevant individual before collecting personal data; such data must pertain to the Network operators' services.
- Expressly set out the reason for, scope and method of collection and use of personal data.
- In the event of a data breach, make a report to the authorities, take necessary remedial steps and inform/notify the relevant affected individuals of the same.
- Review or amend personal data at the request of the relevant individual/user.

With regard to the monitoring of user content, they must:

- Monitor content published by the user.
- Report to the authorities and maintain records of illegal content.
- Remove illegal content.

CIIO are also subject to similar requirements.

Network operators are subject to "mandatory testing and certification". CIIO are also required to sign confidentiality and security agreements with their suppliers of network products and services and assess cybersecurity risks at least once a year.

Enforcement

Network operators and CIIO are required to cooperate fully with and provide access to the enforcement agencies when requested to do so.

The main enforcement authorities are:

- Cyberspace Administration of China ("CAC") which has primary responsibility for the supervision and enforcement of the CSL.
- The Public Security Bureau ("PSB") which has investigatory powers and enforces the CSL at local level.
- The Ministry of Industry and Information Technology which oversees the supervision and protection of personal data by telecom operators and internet information services.

The CAC and PSB are empowered to investigate matters and make the appropriate enforcement orders. There is no opportunity for Network operators or CIIO to make representations at a hearing. If they wish to appeal an order, they must do so through the Chinese Courts.

The majority of cases prosecuted to date by the CAC and the PSB relate to Network operators who have failed to properly manage the data of its users, failed to take necessary measures in protecting the relevant network, breached rules in the collection and use of personal data and the management of the user's identification.

Penalties/Orders

In the event of a breach, the following orders can be made by the enforcement authorities:

- Rectification (which has been the most common order to date)
- Suspension of business during the rectification
- Closure of website/apps or part of business
- Temporary removal of apps or cessation of new user sign up
- Imposition of penalty/fines
  - Individuals can be fined from: RMB5,000 (US$750) to RMB1,000,000 (US$150,000)
  - Breaches of the data localisation provisions (see below) may result in fines against companies of between RMB50,000 and RMB500,000 (US$7,500 - US$75,000)
- Detention
  - Network operators can be subject to five to fifteen days detention for breach of certain provisions.

More than one punitive measure can be taken against a Network operator or CIIO per enforcement action.

Civil claims have also been commenced under the CSL and there have been four published awards to date. These have arisen as a result of incorrect or false information posted online and/or a failure to verify the accuracy of the information on a website as well as the posting of defamatory information and/or graphic images relating to individuals. Damages have been awarded up to RMB40,000 (US$6,000)

Data localisation

On 31 December 2018, Article 37 of the CSL, relating to data localisation will come into effect. The basic requirement under Article 37 is that "personal information" and "important data" collected or produced by CIIO must be stored in China. This is a controversial provision which has been the subject of much criticism. In 2016, a joint statement signed by 40 international business groups sought an amendment to this provision but to no avail.

"Personal information" includes all information (whether in electronic form or otherwise) which individually or combined with other information allows the identification of a natural person. This includes personal information such as the name, date of birth, address, identity card number of the individual, etc. The regulatory authorities retain the right to determine what constitutes "important data". This includes trade secrets, state secrets and other such information which the authorities consider sensitive. This is likely to include information which is political in nature. Subsequent draft rules and guidelines provide that Network operators will also be subject to the data localisation regime (as referred to below).

The draft Guidelines and Measures

The relevant draft rules and guidelines are:

- Draft Measures for Security Assessment of Cross-border Transfer of Personal Information and Important Data ("the Measures"); and
- Draft Guidelines for Data Cross-Border Transfer Security Assessment ("the Guidelines").

Both the Measures and the Guidelines apply to Network operators. The provisions also apply to overseas network providers (even if they do not have a presence or operation in China) who supply products or services to a client base in China. In these circumstances, the overseas Network operator would be considered to be engaged in domestic operation. Domestic operation, under the Guidelines, means one which provides products or services within China.

The Guidelines provide factors which are taken into account to determine whether a foreign company is engaged in domestic operation, such as the currency used for payments and the distribution of products to Chinese companies or Chinese nationals.

Consent

In order to transfer personal information outside China, the prior written or express consent by way of affirmation of the data subject must be obtained by the Network operator. (With regard to the latter, this could involve the simple "click" of a "Yes" or No" button online to denote approval or otherwise.) There are certain circumstances when consent is implied or deemed to have been given, for example, when sending an email internationally, when conducting international calls and when making a cross-border transaction over the internet. There is also an exemption which applies in the event of an emergency where there is a danger to the life or property of the data subject.

Security assessments of data transfers

The Measures require that a self-assessment be conducted by a company which purports to transfer personal information or important data outside China. This will involve the preparation of a transmission plan which contains details of the data transfer. The plan is subject to a 'legal' and 'appropriateness' test. If this criteria is satisfied, the issue of whether the cross-border transfer is "controllable" is then addressed. Such assessment will be monitored by the Chinese regulatory authorities.

In addition to the self-assessment, there is also a second type of security assessment which is conducted by the regulated authorities where material data transfers are involved.

The key triggers for a security assessment by the regulatory authorities of a material data transfer include:

- The personal data relates to more than 500,000 data subjects.
- The size of the data to be exported exceeds 1,000GB.
- The data relates to large-scale engineering projects, defence/military, public health, marine environmental, biochemical and nuclear sectors or involves sensitive geographical information.

- System vulnerabilities and security safeguards for critical information infrastructure or similar information.

Penalties/Orders

Penalties can be imposed upon the company and/or the directly responsible manager.
The fines can range from the following:

- Network operators: RMB50,000 to RMB500,000 (US$7,500 to US$75,000). The directly responsible manager: RMB10,000 to RMB100,000 (US$1,500 to US$15,000).
- CIIOs: RMB50,000 to RMB500,000 (US$7,500 to US$75,000). Directly responsible manager of CIIO: RMB10,000 to RMB100,000 (US$1,500 to US$15,000)

These fines can be combined with orders for suspension of business, revocation of the business licence and/or detention.

Commentary

Multi-national corporations who provide either services or products within China will need to store personal information and important data which has been collected or generated within China and will therefore need to comply with the new Measures and Guidelines. However, at the time of writing these remain in draft form, and a third draft is believed to be in circulation but has not yet been published. Compliance is required by 31 December 2018, when the data transfer regime is due to come into effect. Companies must therefore move swiftly to be ready for this deadline. There are significant challenges ahead and the cost of compliance is likely to be high. In addition, the concept of “important data” continues to be less than precise and will necessarily increase the risk of exposure to criminal and, possibly, civil liability. This is more so the case since the regulatory authorities retain discretion as to how the term “important data” is to be interpreted.

Rosie Ng is a Consultant in the Insurance/Reinsurance Group of HFW. Her main practice comprises of advising policyholders, insurers, reinsurers and intermediaries on all aspects of insurance and reinsurance dispute resolution. In particular, she advises on claims arising out D&O, professional indemnity, commercial crime, fidelity, employment practice liability, product liability, business interruption and construction-related insurance. With regard to non-contentious insurance, she advises on policy wording and product development.

She is qualified in England and Wales and Hong Kong.

She is also a former director of the Hong Kong Insurance Law Association and a regular speaker at market events and contributor to insurance periodicals.

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.

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