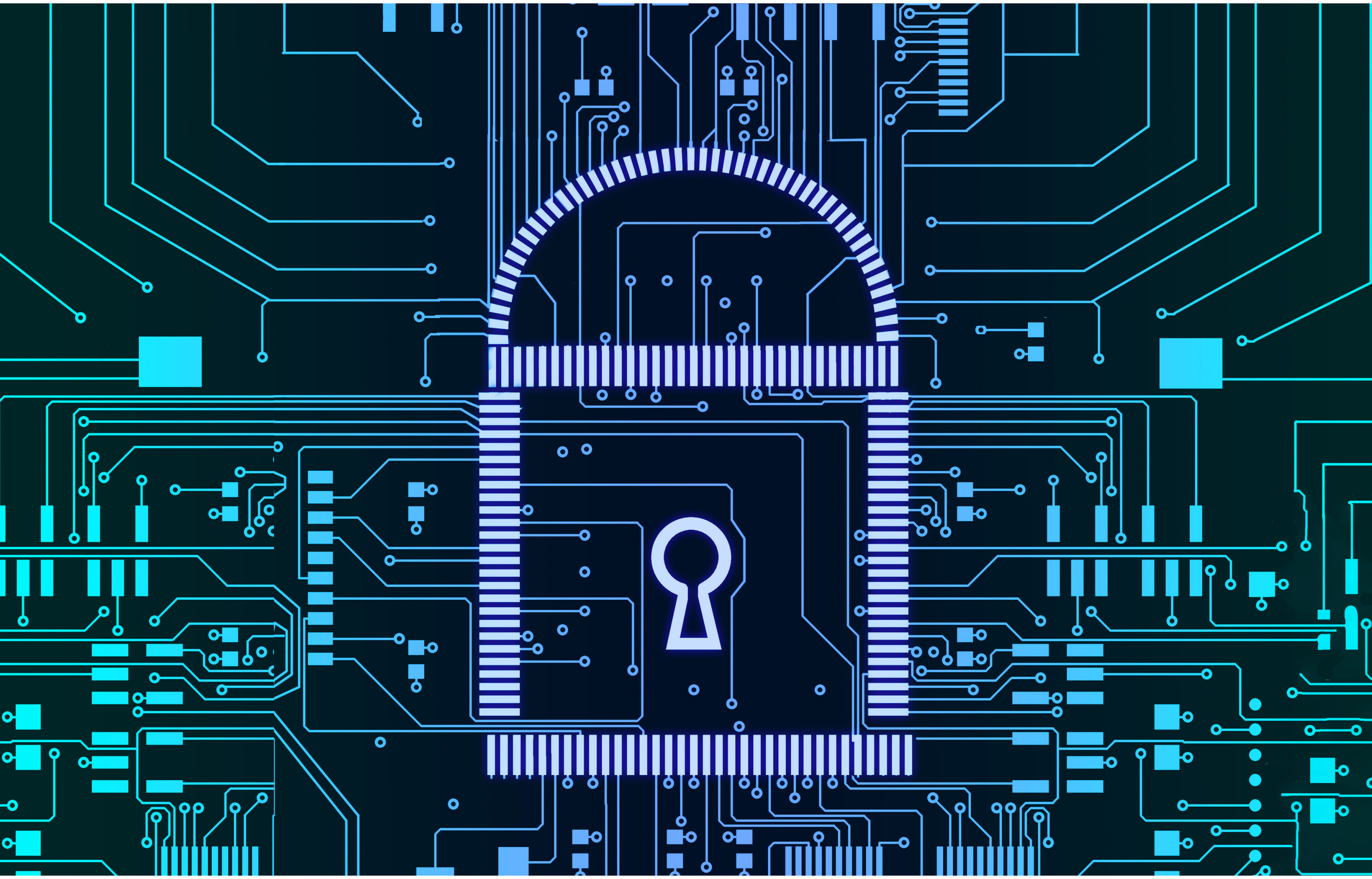
TransReflections

Cyber Newsletter

Winter 2021



TransRe™
We value cyber risk.

Table of Contents

Introduction

2021 has been an eventful year in the cyber (re)insurance market. Ransomware and systemic challenges dominated the headlines. Earlier in the year we wondered if (not when) the escalating trend in ransomware payments would stop. Since then there have been signs of progress. It may be too early to call the $45M payment referenced FinCEN's latest report as the high-water mark, but the Colonial Pipeline attack shone a very public spotlight on the issue, and cyber insurers have tackled ransomware exposures with more discerning risk selection, more in-depth underwriting analysis, more price and lower limits (although $100M facilities do still exist). This marks a significant turning point for the cyber market, after years of chasing premium with ever-enhanced covers and expanding aggregates. As a result, retention ratios have fallen, while overall premiums have grown.

Governments have also been more active this year. France questioned the insurability of cyber extortion payments. A G7 communique urged Russia to take action against ransomware gangs. The US Department of Homeland Security issued a ransomware whitepaper that encouraged dialogue with the cyber insurance industry, and the industry has been reminded (twice) of its anti-money laundering obligations under OFAC. Most encouragingly, we have seen the benefits of public/private collaboration in the partial recovery of some ransomware payments, most publicly as the result of the FBI's blockchain analysis in the Colonial Pipeline case.

We continue to monitor ransomware developments closely. While the cumulative effect of these changes is undoubtedly positive, issues remain. For example, we do not yet know the full impact of more rigorous underwriting on frequency and severity. Is the recent improvement because some bad actors have temporarily paused their activities after the Colonial Pipeline publicity? The threat actor landscape appears as menacing as ever. How severe will the double extortion phenomenon become (extortion to also avoid data exfiltration exposure)? The impact of 3rd party claims will take time to play out. So too the final settlements of some 2020's largest business interruption claims. Many insurers have shed their bottom quartile of risks, but are those risks being re-bound elsewhere without any fixes to their security posture? In other words, is the industry raising the bar to what is deemed insurable? Technology adoption continues apace, which requires increased expenditure by all market participants. It has also resulted in a market split between established carriers with loss experience (who have learned to adapt as a result of paying those claims) and the newer wave of insurtechs who have not had the claims experience, purportedly due to their technical superiority.

Further, ransomware may be the number one priority, but it isn't the only one. We have not had a major insurance systemic event since 2017's NotPetya (which affected multiple classes, not just cyber) but we have seen several scares over the past year. Each time, from SolarWinds onwards, there is a clouded aftermath as severity is assessed, but the loss ratio evidence points to low insurance losses tied to events this year (so far). That may be because the attackers are nation state actors rather than criminal gangs. Or it may be the nature of ransomware claims and the fragmented repositories of loss data make it difficult to identify how many claims resulted from eg the Accellion data breach.

As evidence of progress, we have been encouraged by the demonstrated ability of insurers to review their portfolios for exposure to Microsoft Exchange or Kaseya using internal capabilities or 3rd party vendors, and by their progress in pushing insureds to immediately remediate issues. Both data points show insurers are moving to continuous monitoring in place of traditional, annual underwriting.

Technology will continue to increase its role in assessing portfolio exposures and scoring client risk postures, but technology alone is not sufficient. It seems odd to talk about ransomware and covid-19 positives, but the market has an opportunity to re-consider how much systemic coverage it is willing to offer, and at what price. The first signs are positive: a more robust approach to tracking CBI exposures; the stripping out of too vague un-named supply chain extensions; a wholesale change in underwriting appetite for systemic exposures. Each can be implemented by underwriting teams now, and all will improve the market's long-term resilience against systemic events. Such steps include logical areas of collaboration among market stakeholders, most notably in the formation of CyberAcuView.

The threat landscape remains challenging, but the insurance marketplace is in better shape than it was, and here is to further progress in 2022!

Rhett Hewitt
December 2021

Notable Breaches

Large Insurer Suffers Ransomware And Data Breach Attack

In March 2021, CNA discovered that their systems had been breached in an attack that included a $40M ransom payment. Nearly 75,000 customers had personal data stolen and it was reported that CNA was not able to fully restore its systems until mid-May.

Tokio Marine Experiences Cyberattack

In August 2021, Tokio Marine Insurance Singapore (TMiS) announced they had been the subject of a ransomware cyberattack. The attack was exclusive to TMiS and no customer or confidential information was exposed.

Ryan Specialty Group Investigates Unusual Activity

Insurance broker Ryan Specialty Group began an investigation in August 2021 following unusual activity in April related to employee email accounts. The investigation revealed that personal data was accessible but not accessed during the attack.

AXA Insurance Group Breach Possibly Linked To Insurance Decision

AXA Insurance operations in Thailand, Hong Kong, Malaysia and the Philippines were breached in another ransomware attack that compromised customer records. The company was also hit with a DDoS attack nearly simultaneously. Coincidentally, mere weeks before the attacks, AXA announced that they were dropping coverage for ransomware payments on policies in France.

Florida Water Supply Hacked

An unknown hacker hacked into the water supply of Oldsmar, FI via popular remote-access software provider TeamViewer. The hacker gained control of the water treatment system and altered the settings to increase the amount of sodium hydroxide in the water. A city employee witnessed the attack and immediately returned the settings to normal levels. The city later specified that there are additional safeguards in place.

Cyberattack Disrupts Fuel Supply To US Eastern Seaboard

In May 2021, fuel pipeline operator Colonial Pipeline suffered a breach in their IT systems which affected their ability to operate their network of pipelines. Colonial paid roughly $5M in ransom to regain access to its system. The FBI was involved with the investigation and the Justice Department was able to recover a significant portion of the ransom a month after the attack. Threat actor Darkside claimed responsibility and the group was completely shut down due to actions of the US government. The U.S. Transportation Security Administration issued a new reporting requirement that states pipeline operators must report cyberattacks within 12 hours of occurrence and have a cybersecurity coordinator on call 24/7. Violation of these fines start at $7,000 a day.

UK Engineering Group Hit By Ransomware Attack

Headquartered in Glasgow, Weir Group a FTSE 250 listed company confirmed that they were managing a ransomware attack that occurred in September and caused temporary disruption. The consequences of the operational disruption and associated inefficiencies are expected to continue into the fourth quarter of 2021.

Widespread Impact From Microsoft Exchange Breach

In early 2021, Microsoft Exchange servers were breached using a zero day vulnerability that left tens of thousands of organizations worldwide scrambling to secure their systems. While Microsoft released patches for most of the vulnerabilities in short order, it is unclear how quickly those patches were applied worldwide. Notably, the US took the rare step of formally blaming China for the breach.

US Telecom Company Reports Unauthorized Access

Syniverse, which offers mobile data and other services reported in a recent SEC filing that the company became aware of unauthorized access to its operational and information technology systems in May 2021. The hack originated in May 2016.

Kaseya Breach Affects 1,500 Organizations

Managed services providers (MPS) have long been a worrisome attack vector and Kaseya breach is a perfect example. In July 2021, Kaseya's tech-management software was compromised and threat actor REvil locked down the systems of 1,500 organizations. The ransom demand was $70M and Kaseya claims they did not pay the ransom.

Millions Of T-Mobile Customers' Data Exposed

T-Mobile confirmed its systems were subject to a criminal cyberattack that compromised data of millions of customers, including former and prospective. The mobile network operator is coordinating with law enforcement.

Bangkok Airways Investigates Customer Breach

Thai airline, Bangkok Airways announced that it is investigating a cyberattack that might have exposed passport, historical travel and partial credit card information.

More Death By Ransomware

In 2020, a patient in Düsseldorf was unable to receive life-saving surgery due to a cyberattack. Recently we learned about a similar scenario in Alabama where a newborn was unable to receive needed care during Labor & Delivery and passed away, allegedly due to injuries suffered at birth. Physical damage and death connected to cyber events have been considered a difficult risk from a coverage standpoint due to real-world examples being rare. This viewpoint could change with the recent increase of large-scale ransom attacks.

Regulatory and Legislative Update

Amazon Receives Record EU Fine

Luxembourg's National Commission for Data Protection levied a €746M GDPR fine against Amazon for violating the regulations on processing personal data. Amazon has stated that they will appeal the fine.

EDPB To Increase WhatsApp Fine Over Transparency

The European Data Protection Board (EDPB) issued a final binding decision and fined WhatsApp €225M following a reassessment of draft decision issued by the lead supervisory authority (the Irish Data Protection Commission) to issue an administrative fine between €30M-€50M.The issue stated that WhatsApp had discharged its transparency obligation under GDPR. Eight other European supervisory authorities contested the draft decision.

Employee Performance Algorithms Lead To Italian Fine

Italian data regulator fined food delivery service Foodinho €2.6M for using algorithms to manage employee performance.

Additional US States Enact Consumer Privacy Laws

Virginia and Colorado have recently enacted Consumer Privacy laws similar to California's CCPA or the GDPR. Florida, New Jersey, New York, Oklahoma and Washington have similar bills under consideration. This patchwork of privacy laws continues to expand in the absence of a federal rule. In May 2021, President Biden signed an executive order on "Improving the Nation's Cybersecurity," and followed that order with a National Security Memorandum. In August, he met with Microsoft, Google and insurance industry leaders from Travelers and Coalition and established additional initiatives to improve national cybersecurity and supply chain security.

U.S. Department Of The Treasury Expands Russian Sanctions

In April 2021, the US expanded the sanctions against Russia and several Russian corporations based on their "destabilizing behavior." That behavior includes interference in free and fair elections in the US as well as "engaging in and facilitating malicious cyber activities against the US and its allies and partners." This and a series of other recent actions by the US government demonstrates they are not hesitant to make attributions.

What is Adequacy?

EU publishes UK adequacy decision following Brexit.

Facebook Face Down

Facebook is facing new scrutiny for its business practices as whistleblower Frances Haugen exposes corporate practices in testimony to a Senate subcommittee. Her testimony has been wide-ranging and focuses on the harm that Facebook knowingly does to children, communities and the political system in the US and the lack of concern within the company about the damage.

Litigation News

Illinois' BIPA Statutes Continue To Evolve

American Airlines is fighting to keep the BIPA lawsuit against them in federal court. In April 2021, a $25M settlement was approved to conclude the BIPA class action lawsuit against ADP. There are some BIPA cases that have been put on hold pending the outcome of several appellate cases involving the statute as they might significantly change the landscape.

British Airways Settles Claims For 2018 Data Breach

British Airways has settled a legal claim brought by those affected by the 2018 breach. UK regulator, Information Commissioner's Office (ICO) issued its largest fine (at the time) of £20M to the airline.

Crypto Corner

China bans all crypto transactions

Africrypt a South African Bitcoin investment firm was hacked and lost $3.6B in bitcoin

Poly Network was hacked and had $600M+ stolen, only to be returned by the hacker

Coinbase is facing uproar from customers over lack of response to hacked accounts

Liquid Global loses $97M+ of customer crypto in cyberattack

Binance is being investigated by the U.S. Department of Justice and IRS for money laundering

ION Science Ltd v Persons Unknown and others

The English Court provided remedies for initial coin offering (ICO) fraud. The court granted permission to serve disclosure orders on two cryptocurrency exchanges and implement a worldwide freezing order on persons unknown.

Cyber Publications

Institute for Security + Technology; Ransomware Task Force: Combatting Ransomware

Claroty Biannual ICS Risk & Vulnerability Report:1H 2021

New York DFS Report on the SolarWinds Cyber Espionage Attack and Institutions' Response

OAIC - Notifiable Data Breaches Report: January–June 2021

OFAC – Sanctions Compliance Guidance for the Virtual Currency Industry

FinCen – Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021

SPECIAL GUEST ARTICLE

Put Me in Coach: How a Reexamination of Vendor Management in Cyber Claims can Contribute to Healthier Loss Ratios for the Cyber Insurance Industry.

By: Andrew Lipton, Vice President, Head of Cyber Claims at AmTrust Financial Services, Inc.

First-party Cyber claims present an interesting threshold issue for any cyber claims management professional: which vendors, legal, digital forensics, or otherwise, should be engaged to respond to the claim? For certain types of claims there is no one-size-fits-all answer.

Generally speaking, when an insured submits a first-party cyber claim to its insurance carrier, the cyber claim professional must address the following questions: Has the insured experienced a data breach that will likely lead to notification obligations under applicable law? If so, the insured needs privacy counsel to lead that process. Are we unsure whether a breach has occurred, or exactly what type of data was compromised or stolen as a result of unauthorized network access? If so, the insured needs a specialized digital forensics firm to begin an investigation of the insured's computer system to make any such determinations – moreover, where there is significant risk of future third-party liability to the insured, incorporating legal counsel into the forensic investigation process will increase the chances that the forensic investigation itself will be privileged and protected from discovery by any third party in future litigation.

There are instances, however, where the need to engage legal counsel and/or forensics is not immediately clear for the cyber claims professional. Consider the following cyber claim scenarios:

- An insured reports a lost laptop as a potential data breach – however, all of the data on that laptop is encrypted at the system level, rendering it nearly impossible for any unauthorized party to access the data on that laptop.
- An insured reports that a cloud electronic record service provider is down, and that the provider may have experienced a security incident – however, the insured's systems are otherwise unaffected, and there is no direct evidence of a data breach of the insured yet.
- An insured reports that they were victims of social engineering by way of a business email compromise of one of their customers' systems. The insured's system has not been breached at all – they simply paid money to an unknown party based on a fraudulent payment instruction.

Aside from legal or digital forensics, what services do insureds need when experiencing a cyber incident such as those outlined above? They need "coaching," i.e., incident response advice that helps the insured develop a strategy for remediating that incident. If you ask professionals in the cyber insurance industry, they will tell you that legal counsel usually performs the function of "breach coach" during a cyber claim. Digital forensics firms will also employ case managers that sometimes insert themselves as breach coach on a given claim. Lastly, the cyber claims management professional can also act as breach coach. What results from this dynamic is a shared undertaking of the breach counsel role for the insured – however, this leads to inefficiencies and claim cost creep. That is because two out of the three entities in this scenario engage the coaching role at a cost to the carrier. Is it possible that this leads to higher per-claim cost in cyber insurance generally? If it does, can we start changing the direction of this dynamic, and if so, how?

Clearly, a cyber insurer cannot take on the role of legal counsel or forensic investigator for its insured during the management and adjustment of a cyber claim. Claims professionals can assert themselves more broadly as the primary incident response coordinator as opposed to leaving that role to legal counsel at an additional cost to the carrier.

This is by no means an easy task. It means that cyber claims professionals will have to train and educate themselves on proper incident response procedures and establish their own discrete guidelines on when legal counsel and/or forensic providers should be brought in to service a claim. However, in my view, this is an effort well worth it – even if $1000 is saved on a given claim because non-legal "coaching" services were taken on by the insurer, that could lead to an immense savings when multiplied out in the aggregate over a book of similar claims. The savings is extremely important to everyone in the cyber insurance ecosystem.

That is because policy proceeds saved on a low-severity cyber claim means more policy proceeds available in the same policy year for that Insured when they need it for a higher-severity cyber claim should it occur.

Here are a couple additional ways cyber claim professionals can take a critical look at lowering per-claim vendor costs:

- Have vendors produce itemized budgets within any statement of work submitted to the Insured, and isolate any discrete services that might not be necessary. For example, is the digital forensics firm charging for the deployment of endpoint detection software where it may not be required? What about report drafting when that has not been specifically requested by the carrier or counsel? At a minimum, asking these questions of your vendors will help identify any such unnecessary costs;
- When retaining breach counsel in a situation where only a "suspected" breach has occurred involving a third-party, make it clear to the counsel in question that their services are being engaged for a limited purpose. Keep a close eye on budgets and specifically request an hour-by-hour breakdown of proposed services. Ask critical questions when the hours proposed for certain tasks seem excessive. This is not to be hypercritical of breach counsel, but rather, should serve to solidify the bond of trust between carrier and counsel when it comes to serving the carrier's insureds;
- Lastly – study, study, study. We work in a world where cyber risk changes dynamically. Luckily, there are infinite resources online and elsewhere for cyber claim professionals to dig into and study the technology giving rise to cyber claims. More importantly, take the time to understand what your legal and digital forensic vendors are doing at a subject matter level – if you don't, then you cannot have an informed discussion with them on a claim by claim basis regarding what services are needed, and what services are merely a recommendation.

Cyber carriers and their claims management staff need to strive towards establishing themselves as trusted incident responders for their insureds. Taking a heavier hand in this process will help mitigate against unnecessary policy spend and preserve precious policy dollars for our insured customers.

SPECIAL GUEST ARTICLE 2

China's Personal Information Protection Law

By: Rosie Ng, Partner, Clyde & Co, Insurance/Reinsurance

Introduction

China's Personal Information Protection Law ("**PIPL**") came into effect on 1 November 2021. The PIPL, Cybersecurity Law and Data Security Law (which came into effect on 1st June 2017 and 1 September 2021 respectively) collectively form a three-pillar framework for China's comprehensive data protection and cybersecurity regime. This article highlights the key principles and obligations in relation to the collection, processing and protection of personal data under the PIPL which will impact businesses operating in or doing business with China.

The PIPL

The PIPL governs not only the processing of personal information within China but has extra-territorial effect in the following circumstances:

Where the purpose of the processing of personal information outside China is for:-

- the provision of products and services to natural persons in China
- the analysis/assessment of the behaviour of natural persons in China
- other circumstances as provided for by law and/or regulations.

The PIPL defines '**personal information**' as ***"all information related to identified or identifiable natural persons"*** save for information which is anonymised.

The obligations imposed by the PIPL are upon the '**personal information handler**' which is defined as ***"the organisations and/or individuals who independently determine the processing purpose and method in the processing of personal information"***.

Basic Principles

The PIPL refers to the following Basic Principles in the processing of personal information:

- **The principle of lawfulness, legitimacy, necessity and good faith:** the processing of personal information must not be misleading, fraudulent or coercive. Furthermore, it is restricted to information which is necessary for the relevant purpose
- **Clear and reasonable purpose:** the processing of information must be directly related to a legitimate purpose and the collection of such information must be restricted to all that is necessary for that purpose
- **Transparency:** is required in terms of the rules, purpose, method and scope in the processing of personal information
- **Accuracy:** the collection and retention of information must be accurate, complete and kept up to date
- **Security:** personal information handlers must ensure and take all necessary steps to safeguard the security of all personal information processed by them

Criteria for the processing of all personal information

The PIPL provides that the following conditions must be complied with before personal information may be processed:-

The clear express consent of the relevant individual must be given.

- Such consent must be given on a fully informed and voluntary basis. Separate/ individual consent (as opposed to "bulk" consent) is required in each of the following circumstances:
  - » the provision of personal information to a third party
  - » the processing of "sensitive" personal information
  - » the publication of personal information processed
  - » the use of personal information which has been collected for reasons of public security
  - » the transfer of personal information outside China

Consent can be withdrawn at any time by the relevant individual and the personal information handler is required to set up and provide a convenient mechanism for the withdrawal of such consent

In addition, a personal information handler cannot refuse to provide products/services on the grounds that the relevant individual has refused to give his/her consent or has withdrawn the same unless the processing of such information is necessary for the provision of products/services

- Processing is necessary for the conclusion or performance of a contract with the data subject or for 'Human Resources Management' (i.e. for an employer)
- Processing is necessary for the performance of statutory duties or for compliance with legal obligations
- Processing is necessary for dealing with public health emergencies or for the protection of life or property of natural persons
- Reasonable processing of personal information which has been made public by the individuals/data subjects themselves or through other legal means
- Reasonable processing of personal information relating to matters which are in the public interest such as news reporting and the "supervision" of public opinion
- Other circumstances as provided for by law/ regulations.

Sensitive information

The PIPL affords "sensitive personal information" a higher level of protection since such information, if leaked or used illegally, would cause serious harm to persons/property. The type of information which falls within this category include:

- biometrics
- religious beliefs
- specific designated status
- medical/health
- financial
- personal information relating to minors under 14

Separate consent (as opposed to "bulk" consent) is required before sensitive personal information can be processed. Furthermore, there must be a specific, necessary and legitimate purpose for which processing of the same is necessary. Protective measures to safeguard the security of such information must be taken (which may require requisitioning a Personal Information Protection Impact Assessment). The relevant individuals must be informed of the necessity for processing such information and how this affects his/her rights or interests.

Automated decision-making

Personal information handlers who use personal information for automated decision-making must ensure that:

- the transparency and results of such automated decision-making are "fair and just"
- no unreasonable or differential treatment is afforded to individuals in respect of pricing and/or contractual terms
- where automated decision-making is used in direct marketing with individuals, the personal information handler must provide options which are not tailored to the relevant individual's personal characteristics and there must be a convenient mechanism to opt to refuse

Cross-border transfers of personal information

Under the PIPL, strict conditions must be met before transfer of personal information can be effected outside China. The personal information handler must:

- obtain the individual/data subject's separate informed consent;
- conduct a Personal Information Protection Impact Assessment and make/maintain records
- comply with one or more of the following special conditions:
  - » pass the relevant security assessment laid down by the Cyberspace Administration of China
  - » obtain the relevant certification from a specialised agency
  - » the relevant contract was concluded with a recipient party outside China
  - » comply with other conditions imposed by PRC law/regulations.

Furthermore, the PIPL provides that the express approval of the competent PRC authority must be obtained before personal information stored in China can be transferred to any overseas judicial authorities or agencies.

The governance and security of personal information

Personal information handlers are under strict obligations to safeguard and ensure the security and protection of personal information. Key duties include the following:-

- ensuring that a system is in place which protects personal information from unauthorized access, leakage and loss
- the appointment of a Personal Information Protection Officer ("**PIPO**") who will be accountable and responsible for the supervision of matters and obligations under the PIPL
- where the PIPL has extra-territorial effect, a representative/a designated office in China must be appointed
- Compliance audits are required to be conducted on a regular basis
- Personal Information Protection Impact Assessments must be undertaken before the processing of personal information in certain stated circumstances:
  - » where personal information is to be used for automated decision-making
  - » involves sensitive personal information
  - » where third party providers are instructed to process personal information and/or where there is public disclosure of personal information
  - » where there is cross-border transfer of personal information
  - » where processing personal information will have a significant effect on an individual/data subject's rights

Mandatory reporting of data breaches

The PIPL imposes immediate mandatory reporting of data breaches to the relevant authority on a personal information handler. In

certain circumstances, the affected individuals may need to be informed.

The data breach notification must contain details of the following:

- the type of personal information which is subject of the data breach
- the reason/cause of the leakage, loss or illegal access
- the damage sustained
- remedial measures which have been and will be taken
- mitigation measures
- contact details of the personal information handler

Rights of individuals/data subjects

Data subjects are entitled to the following rights before their personal information handlers can process their personal information:

- details of the name and contact information of the personal information handler
- details of the purpose/method of processing the relevant personal information and period of retention
- details of the procedure by which that individual/data subject can exercise his/her rights under the PIPL
- subject to any laws/regulations to the contrary, to restrict/object to the processing of his/her personal information
- to access and/or copy the relevant personal information
- to correct or rectify the content of his/her personal information
- to request deletion of his/her personal information in certain given circumstances (for example, after withdrawal of consent)

General breaches

The following orders may be made against an individual for breach of the PIPL:

- rectification
- warning
- confiscation in respect of any illegal gains
- suspension/termination of the application programmes which processed such personal information
- fine of an amount not exceeding RMB1 million (USD154,856)
- responsible personnel may be subject to a fine of between RMB10,000 (USD1,548) and RMB100,000 (USD15,485)

Serious breaches

In the case of severe breaches, a fine in the sum of up to a limit of RMB50 million (USD7,742,815) or 5% of the previous year's business revenue can be ordered

Entities/companies may be subject to an order of suspension of activities/closure of business or revocation of their business licence/permit

Responsible personnel are subject to a fine of between RMB100,000 (USD15,485) and RMB1 million (USD154,856); an order can be issued banning such individuals from holding directorships, supervisory or senior managerial positions or to act as a PIPO for a stated period

Conclusion

The PIPL is a significant piece of legislation with far reaching effects. There are parallels to the EU's General Data Protection Regulation. Due to the fact that it applies to data handling activities in China as well as those outside China (in certain stated circumstances), it is critical that corporations take the necessary steps to comply with the stringent requirements of the PIPL.

About Rosie

Rosie Ng is a Partner in the Insurance/Reinsurance Group of Clyde & Co in Hong Kong. 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.

IT Manager Article: It's All About Control

By Neil Inskip, SVP – Systems, International Division – IT, TransRe Europe

In my last article, I wrote about the wildlife outside of my house that both distract and inspire me. There is one other thing that continues to cause me issues while I work from home, a young Border Collie named Skipper. 30 years ago I had the same breed of dog so I have refused dog training because I know what I am doing. However, the reality is that I lack control, mainly when he drags me around the block on his walks. I have five books on training and I have watched multiple YouTube videos. There are logical controls such as voice commands and physical controls such as harnesses, anti-pull collars and treats. If you know which method works best, please write your answers on a postcard.

When it comes to Cyber controls, "SANS" and The Center for Internet Security (CIS) have the answers! In the industry, it's well known that CIS TOP 20 Controls is an excellent starting point for IT teams when it comes to Cyber security controls. Over the years, this list has improved and is on version eight. I won't try to cover all of the controls in this article, but merely highlight some of the major ones.

The top two controls are key to every other subsequent control, essentially how can you begin to defend what you don't know. So, we have to create inventories. Control 1 is "Hardware Assets" and Control 2 is "Software Assets". The next step is to define appropriate controls with the inventories. This is usually a battle ground for Cyber teams because business practitioners want or need the 'new toy' or software package and the security team want as little as possible or at least enough time to sanction it. Ultimately, Cyber teams will essentially make a list of allowable items and block everything else. A passive asset discovery mechanism is useful for this control.

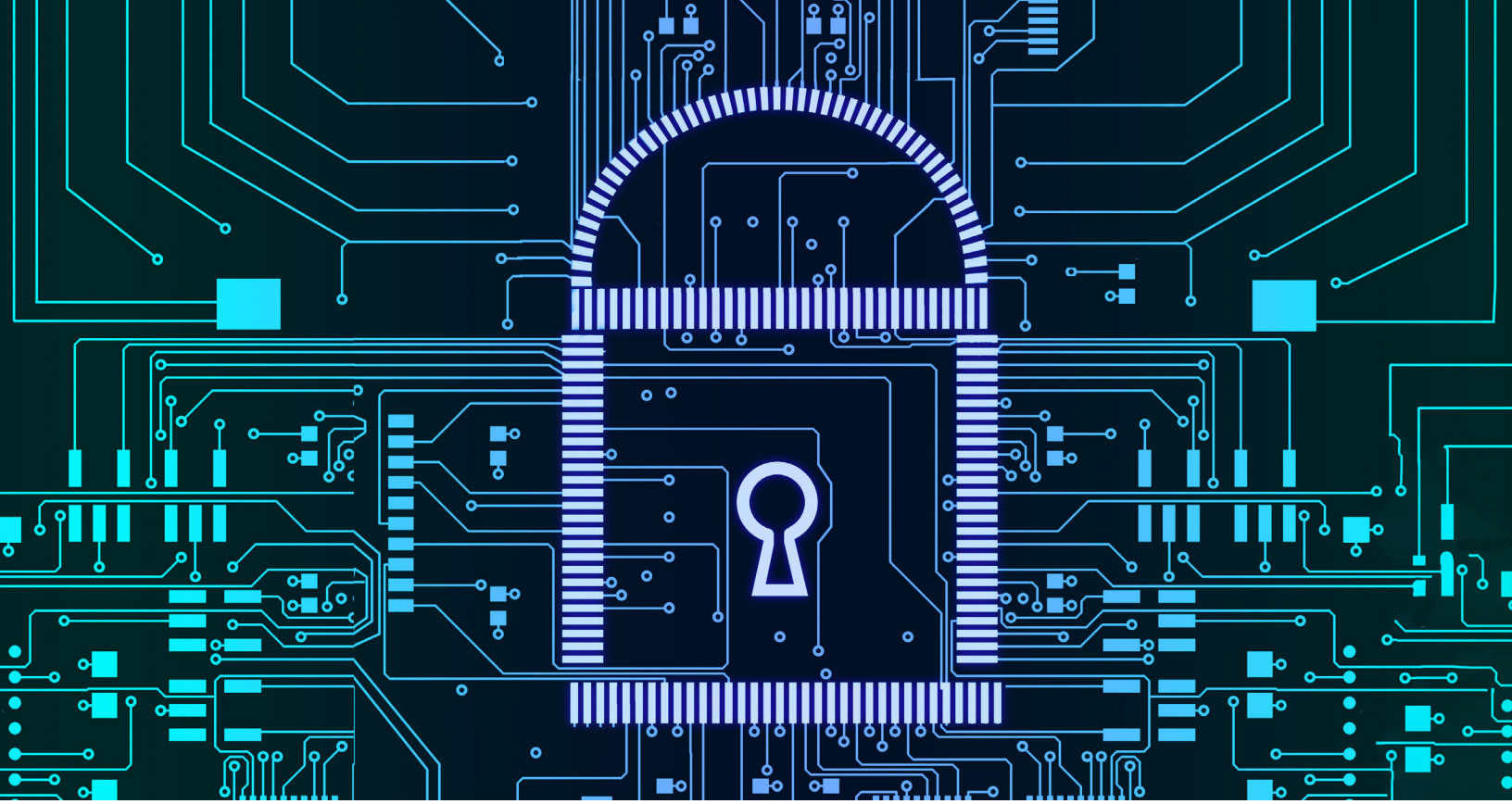
Climbing up our Top 20 "pop chart" and up several places from version 7 is Control 3 "Data Protection" or the development of processes and technical controls to identify, classify, securely handle, retain and dispose of data. This is one of those heavy on people-power topics because it's not just the Cyber team. Legal & Compliance also play a big part in understanding the risks associated with company data. The business staff need to do the ongoing classification and the Cyber team have to provide the technical solutions that wrap around everything.

Control 4 is creating and maintaining secure configurations for the enterprise assets that you discovered in Control 1 and Control 2. This includes processes to do that for all your enterprise assets. Enterprise assets are end user devices (desktop, laptop, tablet, cell phone), IoT devices and servers and all software. There is a lot in Control 4 and you could be thinking "keep it all up to date"? Well yes, but don't forget most devices are shipped with default passwords. After you log on by default, take note whether the system kicks you out or locks the screen after 15 minutes of idle time. In the case of mobile devices, 'can you remotely wipe or find that device'? There are a lot of elements to think about.

Let me tell you what Control 5 is and then I'll let you get back to your day jobs. Control 5 is "Account Management", establish and maintain an inventory of all accounts managed in the enterprise. The inventory should include user and administrator (privileged) accounts. At a minimum, the inventory should contain the person's name, username, any termination date and department name or their manager. These should be recertified on a periodic basis. Control 5 also covers password complexity and multifactor authentication methods, such as Microsoft authenticator, Okta Verify and RSA tokens (others are available). This simply means you are less likely to suffer a credential harvest attack. Any bad actor with your ID and password will need that extra "factor". All of these need a central directory and administration console as well.

Well, we didn't get to the exciting stuff such as vulnerability management, audit log management, email and browser protection and malware protection. I would imagine the CIS are having you focus on the basics etc before you work down the rest of the list which I consider to be very sensible.

Now that I provided some insight, this is probably a good time to stop. Skipper is also barking madly at the front door, so I'll have to sort him out. While it was fun at the time, I'm starting to have second thoughts on whether or not it was a good idea to get him a squeaky toy.



TransRe™
cyber
We value risk.

New York

Underwriting

Miguel Canals
T: 1 212 365 2266
E: mcanals@transre.com

Daniel Hojnowski
T: 1 212 365 2168
E: dhojnowski@transre.com

Actuarial

Joseph Marracello
T: 1 212 365 2159
E: jmarracello@transre.com

Lily Harger
T: 1 212 365 2324
E: lharger@transre.com

Claims

Peter Cridland
T: 1 212 365 2032
E: pcridland@transre.com

London

Underwriting

Rhett Hewitt
T: 44 (0)20 7204 8676
E: rhewitt@transre.com

Claims

Calum Kennedy
T: 44 (0)20 7204 8645
E: ckennedy@transre.com