TransReflections

Cyber Newsletter

3rd Quarter, 2019

TransRe

We value cyber risk.

Table of Contents

3 **QUARTERLY OVERVIEW**
By Elizabeth Geary, TransRe's Global Head of Cyber

4 **NOTABLE BREACHES**
Capital One Data Breach Impacts 100 million+
American Municipalities Targeted, Fighting Back
MegaCortex Ransomware Demands Top USD 5 Million
Hundreds of U.S. Dental Offices Frozen by Ransomware
Russian Pleads Guilty to Hacking Attack
U.S. Delivery Company Breach Affects 4.9 Million
European Aircrafts-Parts Manufacturer Suffers Malicious Intrusion
Airbus Targeted for Commercial Secrets
Malaysian Airline Investigates Data Breach

5 **REGULATORY & LEGISLATIVE UPDATE**
FTC Fines Facebook USD5 Billion
Delaware Enacts Insurance Data Security Act (IDSA)
New York State Adopts SHIELD Law

6 **GLOBAL CYBER SECURITY**
Significant Rise in Targeted Ransomware Attacks
Smart Assistants Are Always Listening
Amazon-owned Ring Doorbells Used by Police
Agent Smith Strikes Worldwide, Asia Hardest Hit
Is the Internet Free?
Alleged Chinese State-Sponsored Attacks on U.S. Utilities
AI Voice Spoofing Tech Used For Fraudulent Transfer

7 **LITIGATION NEWS**
Fed Ex Faces D&O Lawsuit Over NotPetya Impact
Judge in Marriott Data Breach Litigation Orders Release of Investigative Report
US Airline Sues Vendor for 2017 Data Breach
UK Court Rules in Favor of Automatic Facial Recognition (AFR) Technology
European Court Rules In Google's Favor In 'Right To Be Forgotten' Case

8 **CRYPTO CORNER**
Cryptocurrency Exchanges Remain Vulnerable
The Insurance Industry Moves In On Crypto
Cryptocurrency Pricing Remains Volatile

8 **CYBER PUBLICATIONS**
Aon / DLA Piper – The Price of Data Security [insurability of GDPR fines]
Willis Towers Watson – Silent Cyber
Marsh / Microsoft Global Cyber Risk Perception Survey
Guy Carpenter/Cybercube – Looking Beyond The Clouds

8 **TRANSRE SPEAKS**
Where Cyber Exposure Meets The Boardroom – Webinar, Nov 5
Cyber Law & Regulations – Panel Discussion, Nov 6
Emerging Coverage And Claim Trends – Panel Discussion, Dec 6

9 **ZERO TRUST**
By Neil Inskip, TransRe London's IT Manager

10 **CYBER INSURTECH – AN INVESTOR'S PERSPECTIVE**
By Chris Downer and Ken Elefant of Sorenson Ventures

Welcome to our cyber newsletter. We hope you enjoy the articles and updates.

"Who's In Your Wallet?"

When Capital One suffered a hack of the personal and financial data of 100 million customers, the headlines almost wrote themselves. The suspected hacker remains in custody due to an indictment that references thirty other entities (including a state agency, a telecommunications conglomerate and a public research university). It is alleged that the hacks were used at a minimum to access data and to pursue crypto-jacking and crypto-mining activities.

This hacker was caught (tip: don't brag about your exploits online) but hacking (and cybercrime in general) remains an attractive proposition to some: high upside/reward, and low downside/risk of being caught. As a result, individuals, organized crime teams and nation state actors continue to pursue cybercrime. So far it has paid off.

For the companies and municipalities affected, payment may be faster / cheaper (although it still requires time and effort to restore the data / systems if in fact the extortionists provide the key). Over time, the attacks are becoming more sophisticated, and the payments larger.

For cyber insurers, the result is higher attritional loss ratios due to ransom payments, restoration costs, business interruption and loss adjustment expenses. Due to the short timeframes involved – ransoms are paid within a few hours – which means a rise in the frequency and severity of ransom payments will shorten the average cyber insurance tail, if the trend continues.

Insurers are responding by applying pressure to the insureds – all companies are expected to educate their employees, have robust firewalls, back-up systems and processes and to apply them diligently. Some insurers have partnered with firms that offer this service as part of their overall risk mitigation service. Insurers are also raising awareness and rates.

Cyber risk has quickly risen to the top of business concerns. As companies rely more on cloud computing, sensors and analytic tools, companies in all industries must protect their businesses in the digital world just as securely as they do in the physical world.

As cyber security spending reaches new highs, there is a sense of community around the sharing of best practices (and cautionary tales) among employees and consumers, while the justice system plays its part by actively investigating and prosecuting the bad actors.

The tide is turning for cyber insurance. Press coverage about restricted coverage and denied claims has been steadily replaced by more positive reports on cyber hygiene and risk management. Insurance is there when security fails, and the market will grow as part of that wider effort to reduce crime. Cyber underwriting, pricing and claims teams have an important place in the 21st century economy. Who's in your corner?

Elizabeth Geary
Global Head of Cyber

Notable Breaches

Capital One Data Breach Impacts 100 Million+

In July 2019, Capital One announced that a security breach had occurred, exposing sensitive financial data on more than 100 million people in America and 6 million in Canada. The FBI arrested Paige Thompson after she essentially confessed to stealing the data in an online forum. Ms. Thompson had previously worked for Amazon Web Services, where the Cap One data was hosted. It appears she took advantage of a misconfigured server to obtain the data.

> WATCH THIS SPACE: Federal prosecutors claim that Ms. Thompson had "terabytes" of data in her position and that she had intruded on numerous as-yet-unnamed entities. Presumably additional notifications will be coming.

American Municipalities Targeted, Fighting Back

News reports of small (and not so small) American towns being targeted by ransomware have been commonplace in recent months, with cities from Key Biscayne, Florida, to Borger, Texas (one of 22 municipalities in Texas who were hit through a Managed Service Provider), to Lynn, Massachusetts. The U.S. Conference of Mayors met in July and unanimously adopted a resolution not to pay any more ransom demands as it only perpetuates the attacks. The effect the resolution will have on the response to future attacks remains to be seen.

MegaCortex Ransomware Demands Top USD5 Million

An updated version of MegaCortex ransomware has recently hit numerous large corporations across the U.S. and Europe. This relatively-complex ransomware identifies and neutralizes anti-virus solutions that might interfere with the application. It then automatically selects drives/files deemed worthwhile and encrypts them, all without additional action by the bad actors.

Hundreds of U.S. Dental Offices Frozen by Ransomware

Numerous dental offices across the U.S. were infected with ransomware through a shared Managed Service Provider (MSP). In this particular case, DDS Safe, a medical records retention and backup solution was unable to access their patient records. DDS Safe now states "fewer than 100 affected practices were DDS Safe clients…"

Russian Pleads Guilty to Hacking Attack

A Russian has pleaded guilty in the United States District Court of involvement in attacks that compromised the information of over 100 million customers including 83 million of J P Morgan Chase. Others have also been charged with involvement.

U.S. Delivery Company Breach Affects 4.9 Million

Third-party food delivery service DoorDash suffered a breach affecting 4.9 million users and delivery people, compromising their names, physical and email addresses, and some password data. The breach itself appears to have begun in May of 2019 and was discovered sometime in September 2019, although the company did not reveal how long before their announcement the discovery occurred. That question has been a bellwether for how the public and regulators view the breached company.

European Aircraft-Parts Manufacturer Suffers Malicious Intrusion

Belgian aircraft-parts manufacturer Asco temporarily shut down its business operations at offices in Zaventum following a ransomware attack.

Airbus Targeted for Commercial Secrets

A series of attacks earlier this year appear to have been seeking proprietary information on Airbus' A400M military transport aircraft and A350 airline with a suspected link to China. The attacks were launched via suppliers and contractors of Airbus.

Malaysian Airline Investigates Data Breach

Malaysia's Malindo Air, a subsidiary of Indonesia's Lion Air, is investigating a data breach involving the personal data of customers. Up to 30 million passengers of Malindo and its parent may have been affected.

Regulatory & Legislative Update

FTC Fines Facebook USD5 Billion

The U.S. Federal Trade Commission has concluded its investigation into Facebook's privacy violations related to the Cambridge Analytica scandal and has levied a USD5 billion fine, subject to confirmation by the Justice Department. Despite the record-size fine – over 200x higher than the previous record – both politicians and the market seem to view it without concern: one Congressman referred to it as a "slap on the wrist" and Facebook stock closed up 2% after the news broke. Indeed, the company earns roughly USD15 billion per quarter in the U.S. and Canada alone.

> In early September, a totally unsecured database with the Facebook-user identification and personal phone numbers of over 400 million Facebook users was found online.

Delaware Enacts Insurance Data Security Act (IDSA)

Following the NAIC model, Delaware has enacted a new, comprehensive regulatory framework setting forth additional cybersecurity requirements for insurers doing business in the state. Given the disproportionately high number of companies incorporated in the state, Delaware is a significant addition to the roster of NAIC states, joining South Carolina, Ohio, Michigan, Mississippi, Connecticut, New Hampshire, and Alabama in adopting their own versions, generally following the NAIC blueprint. Nevada and Rhode Island have pending legislation to adopt their own versions of the law.

New York State Adopts SHIELD Law

SHIELD, or the Stop Hacks and Improve Electronic Data Security Act for the acronym aficionados, was enacted in July to update the existing 2005 Breach Notification Act. It significantly expands the types of information that, if breached, would trigger a response. It also expands the types of entities covered including expanding the definition of what is considered a "data breach," amongst other additional requirements, to bring the NY law more in line with modern cybersecurity protocol.

OFAC Targets North Korean Cyber Groups

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) recently added three North Korean entities to its list of Specially Designated Nations (SDNs) for alleged malicious cyber activity. The entities included the infamous Lazarus Group which is widely believed to have been behind the WannaCry ransomware attack in 2017.

Sharp Rise in Cyber Incidents in UK Financial Sector

A Freedom of Information request to the Financial Conduct Authority reveals a huge spike in reported cyber incidents to the regulator between 2017 and 2018.

Global Cyber Security

Significant Rise in Targeted Ransomware Attacks

A new white paper from Symantec reports that although overall ransomware attacks are down, targeted ransomware attacks have seen a substantial rise since 2018. These attacks are being led by a handful of hacking groups that have carved the niche out for themselves.

Smart Assistants Are Always Listening

Smart devices including Amazon's Alexa, Apple's Siri, and Google Assistant are always on and always listening. New reports confirm that in some cases actual humans are listening to those recordings, not just a set of computer algorithms. In a world where each of these three systems have sold hundreds of millions of devices that listen to our conversations, it's worth asking the question whether the majority of human conversation is now being recorded.

> Of note, a class action lawsuit has been filed against Google in Illinois, alleging that the collection and storage of voice recordings violates that states' stringent biometrics law, known as BIPA.

Amazon-owned Ring Doorbells Used by Police

Ring Video Doorbells, owned by Amazon, is working with local police departments, coaching them on how to convince residents to agree to let the police use footage from their privately-owned doorbells for law enforcement purposes. All without warrants. Ring also created a "Neighborhood Watch" app where private Ring camera owners are encouraged to share their video footage. Within the Ring/law enforcement partnership, the police are also provided with a special portal that allows them to communicate with and request video from community residents. Further, increasing their use of neighborhood video earns police department credits, which can be used to get free Ring cameras.

Agent Smith Strikes Worldwide, Asia Hardest Hit

Over 20 million devices worldwide were infected with malware dubbed Agent Smith, which replaces apps installed by the user with malicious versions of those apps. The malicious apps then display forced ads to generate revenue. India was the hardest hit country by far, with over 15 million devices infected, with Bangladesh (~2.5M) and Pakistan (~1.6M) rounding out the top three.

Is The Internet Free?

Here are several reminders that much of the "free" internet we take for granted is based on the collection and sale of our collective data:

> Dubbed DataSpii, the process uses extensions available for Chrome or Firefox to collect information on the websites visited by the users, and in some cases, the links available on those webpages and other data from the page. These web histories are then marketed by a now-apparently-defunct fee-for-data company.

> Mental health websites in France, Germany, and the UK mine data, including websites purporting to support those seeking depression help. The data is primarily used for advertising/monetizing purposes.

> Google was fined USD170 million for harvesting data on children under 13 for advertising purposes.

Alleged Chinese State-Sponsored Attacks on U.S. Utilities

In July, at least three U.S. utility companies were targeted with spear-phishing campaigns using similar macros to those used in a previous attack definitively linked to APT10, a hacking group allegedly supported by the Chinese government. It does not appear at this time that any actual control of U.S. utilities was gained, but the discovery of the attempt again raises questions on how war exclusions might come into play if damage is done by a quasi-state actor.

AI Voice-Spoofing Tech Used For Fraudulent Transfer

The CEO of a UK based company was persuaded to transfer USD240,000 to a Hungarian supplier when AI-based software was used to impersonate the voice of the CEO of the German parent company. A second attempt to extract a further payment was thwarted when the UK CEO became suspicious. This incident reminds us of the importance of multi-tiered verification processes in financial transactions.

Litigation News

Fed Ex Faces D&O Lawsuit Over NotPetya Impact

Since the rise of large-scale cyberattacks, the specter of management liability has hovered in the background. It now appears to become increasingly a real threat. As a follow up to last quarter's note, Fed Ex is one such case. Fed Ex acquired a European company called TNT Express NV not long before the June 2017 NotPetya virus impacted large swaths of Europe. At that time, Fed Ex was significantly impacted by NotPetya. The lawsuit alleges that despite the significant impact, the Directors & Officers of Fed Ex "continually assured investors…[that] any negative impact from the attack was minimal…" It wasn't until December 2018 that the full extent of the impact was revealed to investors, resulting in a 12.2% stock drop the day after quarterly results were announced. As demonstrated here – and previously in the Yahoo! and Equifax cases - the potential for increased D&O risk is yet another reason for executive teams to be proactive on cybersecurity and have a response plan in place.

Judge In Marriott Data Breach Litigation Orders Release Of Investigative Report

The federal judge overseeing the Marriott Data Breach Litigation has ordered the release of a detailed report by forensic investigators into how the breach occurred and why it went undetected for years (known as the Payment Card Industry Forensic Investigative Report (PFI) report). Its discovery has previously been attempted in class actions suits without success, apart from heavily redacted versions. Only "narrowly tailored redactions" will be allowed in the case.

US Airline Sues Vendor For 2017 Data Breach

Delta Airlines has commenced a lawsuit against a vendor that provided a chat function on its website. The action against [24]7.ai Inc was commenced in the US District Court for the Southern District of New York, seeking millions of dollars in damages for a data breach that compromised over 800,000 customer records. The airline alleges lax cyber security.

UK Court Rules In Favor Of Automatic Facial Recognition (AFR) Technology

The England & Wales High Court has ruled that the usage of AFR technology in a trial by South Wales police was lawful. The technology processes facial biometrics of the individual for comparison with images on a database and involves large scale and relatively indiscriminate processing of personal data. The matter was considered under both the European Convention on Human Rights and the Data Protection Acts of 1998 and 2018. The courts held that the use of AFR here was not disproportionate and that data was processed in accordance with data protection principals.

European Court Rules In Google's Favor On 'right to be forgotten' Case

In a case that stemmed from a fine issued to Google by the French data protection regulator (CNIL), the CJEU has held that a search engine operator is only required to de-reference for versions of the search engine within the EU and, therefore, the same personal data may still be accessed for domains outside the EU.

Crypto Corner

Cryptocurrency Exchanges Remain Vulnerable

While cryptocurrency enjoys a reputation for secure transactions, its "banking" abilities have proven far more vulnerable.

- CipherTrace reports that through just the first half of 2019, thefts, scams, and misappropriation of funds in the cryptocurrency space have totaled approximately USD4.26 billion.
- Who is profiting from all that theft? Reports indicate North Korea has stolen USD2 billion from its cyber activities, funneling much of the money to fund their nuclear program.
- 3.5 billion yen (~USD32 million) was stolen from Japanese exchange Bitpoint in July.
- Elsewhere, the operator of WeExchange and Bitfunder.com was sentenced to 14 months in prison for deceiving users of those services about the theft/misappropriation of their cryptocurrency, and then lying to regulators about the exploit.
- In Singapore, Bitrue lost over $4 million of cryptocurrency after hackers exploited a vulnerability on one of its internal processes.

The Insurance Industry Moves In On Crypto

Where there is uncertainty, there is a need for insurance. With all the uncertainty noted above, the cryptocurrency field is in dire need of insurance. After a slow start, the insurance industry led by Aon, Lloyd's, and others, is poised to fill that need.

Cryptocurrency Pricing Remains Volatile

As ever, the value of cryptocurrency has been volatile over the last quarter. As of this writing, Bitcoin remains in the USD9,000 range (between ~$9,400 and ~$10,200 in the last month), and Ethereum in the high $100's (between ~$160 - ~$210 in the last month). Most major crypto currencies remain well above their early-2019 low.

Cyber Publications

Aon / DLA Piper – The Price of Data Security [insurability of GDPR fines]

Willis Towers Watson – Silent Cyber

Marsh / Microsoft Global Cyber Risk Perception Survey

Guy Carpenter/Cybercube: Looking Beyond The Clouds, A US Cyber Insurance Industry Catastrophe Loss Study

Cry Cyber And Let Slip The Dogs Of War

TransRe Speaks!

November 5th Where Cyber Exposure Meets The Boardroom **Peter Cridland** and **Seth Goldberg** of TransRe will co-host a webinar with law firm Goldberg Segalla on the increasing D&O risk posed by cyber.

November 6th Peter Cridland will appear on a panel sponsored by the Queens Chamber of Commerce, to discuss Cyber Laws and Regulations

December 4th-6th Elizabeth Geary will join a panel to discuss Emerging Coverage and Claim Trends at the International Cyber Risk Management Conference (ICRMC).

Zero Trust

By Neil Inskip, TransRe London's IT Manager

When IT service companies started to spring up in the 1990's, some networks were only used by IT people. As such, they were not really taken that seriously. For example, one company named their servers after Star Trek characters. If you wanted to access a file, you attached to the "Kirk" server or if you wanted to print a document, you connected to the "Spock" server. All very difficult to remember. When they ran out of core character names, they started using "Security Guard in Red #1", #2, #3, etc. As you can imagine - like the TV show - those guys didn't seem to last too long after they were "beamed down". Apparently, they soon adopted a more sensible approach. Back then there was not too much technology to help and less cybercrime, so generally they had no security and trusted everyone.

If we consider the conventional approach to network security, we just see our internal network as a fortress, with high walls around it. We were happy to let the people inside roam around at will. However, like the movies, if someone crawls down the sewage pipe and enters the fortress via the privy, they have access to the whole of the building, and that's not good.

Some of our readers may have heard of Zero Trust or the Zero Trust Framework, which incorporates a few core principles and technological solutions. But in short, these things combine to form the mantra of "We trust nothing", be that a person or device, coming from or going to, anywhere.

The first principle is to verify the user, to make sure it is the right person. Here we generally apply the use of "Multi-factor authentication" (MFA). MFA is really just saying "give me more evidence it's the actual living person trying to gain access". Most people will be familiar with access tokens used in the banking world that rotate random numbers or websites that will send you a text message if you sign-on from a new PC or device. With companies adopting the use of cloud technologies off premises this requirement is even more important. Once we've verified the person, the second principle, which is not new and forms the cornerstone of IT access and permission, is called "least-privilege". People are given the minimal amount of access needed to do their job. Then, by default, they are denied access to anything they do not need to access.

Those previous two principles are about the person or user. What about network and devices? Firstly, let's talk about the network. Think back to the fortress. There you probably only had two segmented access areas, the general fortress for the general population (the peasants) and the "Keep", the more secure building in the middle where the King and Queen live. What zero trust says is that we should microsegment our networks, essentially build lots of little networks, so we can limit access to just those a person or device needs to access. So, if you only need access to segment A, you don't get access to segment B, where we store all the top-secret documents. We need to understand the data traffic flows and make sure they are aligned to our business flows and processes, and then enforce the policies. Devices you can verify and limit by using various security mechanisms make sure all endpoints are sanctioned by your network access controller.

One major difference with Zero Trust is that the network is built from the inside-out. Once all the requirements are in place, you need centralized management and visibility of the whole thing to monitor end to end and continue to make improvements as required. Indeed, a pivotal facet of Zero Trust is the inspection and logging of all traffic on your network, enabling the IT department to form a working group to review changes to the business requirements.

The above are some core requirements on the web. If you are so inclined, there is also a wealth of material around "Zero Trust" to provide extra color.

Apologies for the shorter than usual piece this time, Fred's backup is failing and Barny needs a reboot, before I can set about installing Betty & Wilma - which is a joke by the way. We don't actually use Flintstone's characters for our server names at TransRe. It's just another example of one of the more unusual server naming conventions I've witnessed being used in our industry.

Cyber Insurtech – An Investor's Perspective

Guest Column By:
Chris Downer and Ken Elefant of Sorenson Ventures

Why It Matters

Earlier this year, the Cyber Risk Management (CyRiM) project (led by Nanyang Technological University and supported by a panel of insurers and reinsurers) issued a report on the potential impact of a cyber breach: "Bashe Attack – Global infection by contagious malware." [1]

The report shows that economic damage to the world economy from a concerted global cyberattack propagated via malicious email could range from $85 billion (in the least severe scenario variant) to $193 billion (in the most severe scenario variant). The total claims paid by the insurance industry would range from $10 billion to $27 billion (where the loss of data from the malware triggers additional claims of data and software loss). Those are some eye-watering numbers. Most importantly, however, is the fact that the estimated 2019 cyber affirmative insurance premium globally is $6.4 billion, which puts the insurance industry loss estimates at 1.2 to 3.4 times the annual insurance premiums. It is an understatement to say that the insurance industry is significantly exposed to a contagious malware event.

Setting the stage in insurtech

Insurtech's visibility and mindshare has grown exponentially since 2015. According to CB Insights data, the four years prior to 2015 (2011-2014), saw approximately $1.5 billion invested in insurance technology deals in aggregate. Since then, each individual year has surpassed that $1.5 billion mark. Last year saw over $4.2 billion invested in over 360 insurtech deals. 2019 is on pace to exceed 2018's record numbers with $3.1 billion already invested across 207 insurtech deals through June 30 (CB Insights Data).

As investment has increased in the space, so too has participation from strategic investors. 2014 saw just 15% of insurtech deals include strategic participation. 2018 saw 43% of deals include strategic participation (CB Insights Data). The trajectory of increased strategic participation has been critical. Certainly, the insurtech movement would not have the scale and momentum without incumbent investment.

While the insurtech movement is very much a global phenomenon, the U.S. has received the lion's share of funding so far. Since 2012, U.S. deals have accounted for nearly 60% of all insurtech deals. France and China are tied for second over this same period with just 9% each of all insurtech deals.

So where does cyber stand?

First let's take a look at the cyber insurance market. Cyber remains a source of growth for U.S. property/casualty insurers, but that growth is slowing. According to Fitch Ratings, the industry's total direct written cyber premiums grew 8% in 2018 to $2 billion, down from 37% growth in 2017. "Year-over-year, there are more buyers than there used to be, which is a trend in the right direction," says Tim Francis, enterprise cyber lead at Travelers, "but there is still an awful lot of the market that does not buy cyber for one reason or another". [2]

Meghan Hannes, U.S. cyber product head at specialty insurer Hiscox, says the company's 2019 Hiscox Cyber Readiness Report found that 53% of U.S. businesses reported a cyberattack in the previous 12 months (up from 38% the previous year), with 45% of those companies experiencing three or more attacks in the past year. "Despite these alarming trends, 27% of firms have no plans to adopt cyber insurance," Hannes explained.

On the carrier side, cyber has, to date, shown strong profitability. Statutory industry direct loss ratios for standalone policies remained. On the carrier side, cyber has, to date, shown strong profitability. Statutory industry direct loss ratios for standalone policies remained consistently favorable at 34% in 2018 from 35% in 2017.[3] Further, market concentration in U.S. cyber insurance remains relatively concentrated with the top 10 writers holding 71% market share in 2018.

What does this mean for insurtechs focused on the cyber problem?

For now, Insurtechs are stuck selling into a concentrated market where the participants are proving to be pretty good at what they do. Are incumbents willing to spend money on meaningful contracts for small business lines that are already profitable? It is a tough place to be.

Insurtechs that have generated the greatest traction (from a funding perspective) within the cyber space have generally been MGAs focused on writing cyber risk. High profile cyber MGAs such as At-Bay and Coalition Cyber have raised $19 million and $50 million total respectively. Each looks to provide risk management solutions for businesses while selling cyber insurance policies to them. Venture investors have flocked to these kinds of companies hoping that they will be able to tap into the nascent cyber insurance market.

While the cyber insurtech market remains young, we have seen one high profile exit to date, in which Guidewire acquired Cyence for $265 million. Cyence's system combined data science, cybersecurity and economic analysis to help financial services firms prospect and select risks, assess and price risks, manage portfolio risk accumulations, and bring new insurance products to market. Guidewire paid a hefty price, outlets reported a Price/Sales multiple of 18x for Cyence.[4]

So, where does the opportunity for venture investors interested in the cyber insurance market go from here?

From our perspective, incumbent enablement is critical for success. When the insurtech movement first launched, a common theme amongst plucky insurtechs was they were out to disrupt and dethrone the incumbents in the space. You couldn't get far into an insurtech presentation without seeing the statement "insurance sucks." This adversarial relationship between insurtech and incumbent was short lived. Today, both insurtechs and incumbents recognize that the insurtech movement can be mutually beneficial. It is no longer a zero-sum game. Enablement of the existing ecosystem – the established carriers - is the key.

In underwriting, for example, there has been an explosion of new data sources over the last several years. While this fountain of new data has the promise to significantly impact the future of underwriting, underwriters often do not have the ability to pull these new data sources into existing processes. In underwriting, the bar for usability is high and the time frame to impact is long – at least a year or two. Therefore, insurtechs must design their data with current underwriting guidelines in mind, while focusing on providing higher quality data that plugs directly into existing workflows. The success of data in underwriting today is based on easy ingestion, data quality, and predictive power (which you can shortcut by focusing on existing attributes).

Differentiation is another key element. The vast majority of cyber-focused insurtech companies look to provide cyber risk scores to aid the underwriting process. Unfortunately, there is often little differentiation between these products, because all rely on open source data and have little proprietary information/data sources. As investors, we are highly focused on companies that can drive competitive moats within their markets, whether that is through IP, a strong team, industry connects, etc. Therefore, to get us excited, we need to see a standout player and not simply a follower. Why is your company the company that is going to succeed? What is it about your team, technology or go-to-market strategy that makes this an opportunity we can't miss?

Those involved in the insurance technology wave have many reasons to be excited about cyber insurance and startups focused on improving risk underwriting. However, patience will be key as new ventures look to tackle this incredibly dynamic market. We expect the space to heat up. Luckily for entrepreneurs with a unique understanding of the industry, we believe there will be considerable appetite for solutions going forward.

About The Authors

Sorenson Ventures *is an early stage venture capital firm focused on software and security investments.*

Ken Elefant *is a Managing Director at Sorenson Ventures. Prior to Sorenson Ventures, Ken was an investor at Intel Capital, Lightspeed and Battery Ventures. Ken has invested in companies such as DocuSign, Forescout, Carbon Black, and AlienVault. Ken has a BS degree from Wharton Undergrad and an MBA from Harvard Business School.*

Chris Downer *is a Principal at Sorenson Ventures. Prior to joining Sorenson Ventures, he was a Principal at XL Innovate focusing on early-stage analytics and insurtech investments. Chris started his career at Goldman Sachs. He graduated magna cum laude from Dartmouth College.*

Sources

1. Bashe attack Global infection by contagious malware
2. Cyber Insurance Market Update 2019
3. Cyber Insurance Growth Slowed in Reaching $2 Billion in 2018, Says Fitch
4. Guidewire Software To Acquire Cyence For Risk Analytics

TransRe
We value risk.

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

Our relationships are based on years of trust and experience. We have a flat organizational structure that combines 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
cyber
We value risk.

	Underwriting	Actuarial	Claims
New York	**Elizabeth Geary** **T:** 1 212 365 2243 **E:** egeary@transre.com	**Joseph Marracello** **T:** 1 212 365 2159 **E:** jmarracello@transre.com	**Peter Cridland** **T:** 1 212 365 2032 **E:** pcridland@transre.com
	Miguel Canals **T:** 1 212 365 2266 **E:** mcanals@transre.com		
	Alex Bustillo **T:** 1 212 365 2376 **E:** abustillo@transre.com		
London	**Rhett Hewitt** **T:** 44 (0)20 7204 8676 **E:** rhewitt@transre.com		**Calum Kennedy** **T:** 0207 204 8645 **E:** ckennedy@transre.com