SPECIAL CYBER EDITION

IRUA JOURNAL OF REINSURANCE

2016 | VOLUME 23 | NUMBER 2

INTRODUCTION

This edition marks a departure from our standard practice of offering a variety of topics and is something of an experiment on which we would much appreciate your feedback. IRUA has entered the twittersphere so you are welcome to contact us that way – **@IRUANEWS** – or through the more traditional email route.

So, this edition is devoted solely to the emerging (or has it emerged?) risk and exposure to **CYBER**. We have a varied range of articles that complement each other and at the same time will both educate and interest you in this rather scary risk.

Since we are first and foremost a reinsurance association we start from a reinsurance viewpoint. TransRe's Kara Owens,who is based in New York City, is ably qualified to expound on cyber as she is in the frontline every day in her role as Global Head of Cyber Risk. The title of her article: **Proceed With Caution: Cyber Ahead** really says it all as, almost, each day brings some news, rarely good, involving cyber. Ms. Owens pithy treatise is a primer on how reinsurers should be aware of these exposures and be pro-active in handling this rapidly growing product line. One of her many interesting points is the capturing and coding of insured cyber-risk exposures and the challenges that leads to for reinsurers. Also, in an industry accustomed to a pretty clear delineation between first and third-party exposures, Miss Owens explains how cyber losses can blur this distinction and create issues for aggregation potential.

Cyber and Big Data go together like peanut butter and jelly etc. etc. so Mark McLaughlin's paper entitled: **Big Data, Big Chances: Effectively Securing Technology, Data... And People** is a great technical expose on the fascinating subject of Big Data and how it has become a key component in current business practices globally and across all industries. Mr. McLaughlin is an insurance industry veteran currently serving as Global Insurance Director of IBM. He works with insurers on many levels predicting trends and developing solutions. Insurers have long been accustomed to working with huge amounts of data, and, especially in the past 20 or so years, so have reinsurers as disaster scenarios and models have become a standard part of underwriting. Modeling has expanded into many more extreme event scenarios and none of it would be possible without what is now known as Big Data. Where there is a mass of data, inevitably, there arises the risk of a cyber-attack and Mr. McLaughlin's article discusses what protective measures companies can, and should, implement including the consideration of purchasing insurance coverage.

Modeling is a perfect lead-in for John Ferrara's article: **Cyber Risk Exposure as It Concerns Data and Actuarial Modeling.** Mr.Ferrara is a Senior Manager at Ernst & Young and works with many reinsurance clients. In his 24 year industry career, among others, he has served as the Chief Actuary for both QBE and JLT Re. Mr. Ferrara covers the subject from a societal as well as an insurance view starting with risk quantification and identification and the types of exposures against which an insured could possibly purchase coverage. Actuarial models are in the development stage and he acknowledges the challenges actuaries face regarding the lack of related available data and the rapidly evolving, and varied, cyber-crime exposures.

Both Messrs. McLaughlin and Ferrara were faculty members at the IRUA seminar held in March entitled: *Claims and Underwriting Aspects of Emerging Risks* and their presentations, while not necessarily the same as included here, sowed the seed for this special JOR edition.

Finally, we return to the insurance company world and include a tour de force from Aspen Insurance's Oliver Brew entitled: **Cyber Risk and The Evolution of Supply Chains.** Mr. Brew is based in London and holds the title of Global Head of Cyber Risk and Head of International Professional Liability, Technology and Cyber Risk.

Supply chains are a fact of life for most manufacturing businesses and a major cyber-attack could have devastating results not only for the supplier but also much further upstream in the chain to the point where, in comparison, the Thai floods in October 2013 and 2011 Tohoku earthquake disruption could be viewed as modest losses. With minor modifications to fit our format, this article was published by Mr. Brew and the Aspen team as an Aspen White Paper and is available on their website. The paper covers the subject so comprehensively and incorporates so many areas of cyber interest that it rounds out our special edition especially well.

On to IRUA news. We are pleased to welcome **a new member to the *Journal of Reinsurance* Industry Advisory Panel.** A. Lindsay Doering has joined the Panel and holds the distinction of being a former JOR author from way back in 2000. Mr. Doering career spans both insurance and reinsurance and, most recently, he was with Chubb & Son, Inc. as a Senior Attorney in the General Counsel Department. That said, his role there mainly involved advice and counsel on matters relating to reinsurance transactions and claims. Welcome, Lindsay!

Our **new website** is progressing well and is at the tail end of development. Updated content is being added as fast as we can produce it. As hinted at in the prior edition, the new, searchable, **database of all JOR articles** going back to the initial Vol.1 No.1 in the Fall of 1993 is complete and will be loaded onto our test site soon. Access to this database of 370 individual articles constitutes, an additional benefit of IRUA membership and for our JOR subscribers a valuable benefit and all for a modest annual subscription fee!

IRUA's 50th Anniversary Conference program is coming along nicely -- so save the dates of **April 5-7, 2017** to celebrate and join us at the PGA National in Palm Beach Gardens, Florida. More information will be posted on our website at **www.irua.com** as it becomes available so please check our website frequently – as the exciting new one is scheduled for a September rollout.

Best regards,

Jerry Wallis, IRUA Executive Director

Intermediaries & Reinsurance Underwriters Association

Vision

To facilitate a vibrant forum that encourages professional and personal development of member company personnel through educational excellence, the exchange of knowledge among industry constituents within the insurance and reinsurance marketplace and recognition for academic excellence for the next generation of reinsurance professionals. We accomplish this vision through focused educational offerings, a robust Scholars program, the publication of the *Journal of Reinsurance,* and an annual Conference.

Mission Statement

The IRUA is a not-for-profit corporation, organized for the purpose of providing high-quality insurance and reinsurance education, meaningful networking opportunities, and the dissemination of topical publications and information relevant to the reinsurance industry.

PROCEED WITH CAUTION: CYBER AHEAD

BY KARA OWENS, TRANSRE

About the Author: Kara Owens is Global Head of Cyber Risk at, TransRe based in New York. Prior to TransRe she was with Guy Carpenter, also in New York. She is active in the US Re Under 40s Group, Association of Professional Insurance Women and engages in substantial charity work. She is a graduate of Temple University's Fox School of Business and Management and holds the following professional designations: CPCU, RPLU, ARe, ARM and AIS. Recently, she was appointed a board member of the Cyber Risk Management (CyRiM) Project, an initiative of Nanyang Technological University and supported by the Singapore Monetary Authority, the Cyber Security Agency of Singapore, and five industry partners, including TransRe.

Abstract: Combine a lack of historical data, differences in policy wordings and few legal precedents. Mix in existing aggregation issues and ever-broadening coverage. Looking back doesn't offer a clear route to the future of cyber insurance – the path forward can be profitable, if the major potholes are avoided..

OBJECTS IN THE REAR VIEW MIRROR

From a reinsurer's perspective, cyber risk presents something of a dilemma. Cyber insurance is a growing product line, with accelerating premium projections supported by the continuous publicity surrounding the issue. To date, our industry's results have been profitable. However, there are enough warning signs visible to suggest that past performance is not a guarantee of future returns. The path to profitable cyber coverages is not a self-driving car – it requires underwriting, actuarial, accumulation management, and claims expertise to steer.

GET PAID FOR WHAT YOU COVER

Lloyd's recently published a cyber strategy paper that highlighted the need to avoid giving away cyber coverage free as part of other standard policy wordings. Passive cyber coverage is like passive smoking – it took many years before the dangers were fully understood, but it can do just as much harm. There should be no such thing as 'free' coverage: insurers and reinsurers need to understand that cyber risks can arise in policies other than traditional cyber products. Today, there are many product lines where cyber is not explicitly excluded which can lead to uncertainty and create an ideal canvas for court arguments. As an industry, we must seek to cover clearly identified, quantified and priced cyber coverage. A large scale cyber-attack will not be restricted to one or two product lines – it may have universal implications.

GET THE DATA YOU NEED

Although cyber insurance is not a new product, many of today's policy providers don't have a long track record of data. Even those who do face a number of challenges – the landscape today is unrecognizable from the mid-90s when 'cyber' products were first launched. This is an exceedingly fast moving arena, where attention is driven by the imagination of the attackers combined with the size of new headlines. After the Target and Home Depot cyber infiltrations, retailers topped the list of underwriting concerns. Today's discussions center on healthcare, energy and utility infrastructure. In terms of how the attacks take place, fear of "Point-of-Sales" terminals (swiping a card – how quaint) has been nearly replaced by ransomware and CEO scams.

Not only does the rapidly shifting terrain render last year's 'treasured' data almost worthless: despite all the headlines to the contrary there have been few catastrophic events to date. This lack of data, particularly around severe events, makes the task of pricing cyber risk in an actuarially valid way extremely challenging. The absence of data is compensated for by assumptions, which vary by company to such an extent that we have seen insurance towers with inverted pricing: a carrier attaching higher in the tower is getting more rate than a carrier in the middle, despite the latter being closer to the risk. Inverted pricing, like inverted bond

CONTINUED ON PAGE 4

PROCEED WITH CAUTION: CYBER AHEAD

CONTINUED FROM PAGE 3

yields, is a signal. In this case, it signals a lack of clarity, certainty and therefore understanding.

How cyber data is captured and coded has changed over the years. At one time, the data was coded as technology E&O. As systems improve, and awareness increases, the level of detail is better, but we still struggle to extract cyber data from blended policies such as Miscellaneous Professional Liability. If insurers do not code and capture the exposure data, then it affects what they are able to provide when they seek reinsurance protection. If insurers are able to provide better data to reinsurers (including a clear split of first and third party coverages) that will lead to more clarity and enhanced reinsurance support. We have also seen numerous examples of limited cyber coverage included in property, traditional casualty and other treaty lines. Without accurate data, we are forced to rely on (conservative) actuarial assumptions in our pricing. This lack of clarity surrounding data can cause increased assumptions of risks, which in turn will fuel the aggregation issue.

If insurers buy a separate reinsurance treaty for their cyber portfolios, then the incentive to capture and analyze the data is reflected in the price of the protection. Fewer assumptions lead to better prices.

POLICY STANDARDS WOULD HELP

To date we do not have a standard cyber ISO form. Cyber carriers use different policy forms. Some have multiple policy forms, and update them frequently. The terminology varies and manuscripting is common for larger/more complex risks. Sub-limits for different coverages are common, which introduces the understanding of drop-down exposure to the mix. All of these factors make it difficult for reinsurers to identify and understand what is being reinsured.

More insurers are offering more coverage, adding physical damage and bodily injuries to the 'traditional' 1st & 3rd party cover. While this demonstrates a clear demand for additional protection, it also adds to the uncertainty: is cyber covered under other standard forms such as property? In an ideal world, these expanded covers would be included in a standardized, standalone cyber policy where they could be properly underwritten, understood and priced. Conversely, they would be clearly excluded from all other product line policies and reinsurance contracts. The alternative is a systemic issue across multiple portfolios in the case of a large event, with insurers not knowing what's covered by what policy, nor what's protected by what reinsurance contract.

LEGAL PRECEDENTS WILL HELP

Legal precedents offer the ultimate rear view mirror, but the view is only partial. Most precedents so far have been around 1st party liability - and just because your information has been accessed does not mean that you have actually suffered harm. Typically, if money is taken from an individual/consumer's account, your bank will reimburse you for any fraudulent activity; however, if you are a small or mid-size business and your bank account has been hacked, you may not have the same protections, or be so readily compensated. Attorneys have also struggled (so far) to consistently prove standing for 3rd party elements. Once they do, claims activity (and precedent data) will increase.

To date, there have been very few settlements when defendants reimbursed credit card companies for the costs of a breach. In most of these cases, the size of the losses had already exhausted entire insurance towers, leaving insureds to absorb the 3rd party costs that may have triggered the policy. As customers react, and buy larger towers, so the insured losses (1st and 3rd party) will surely grow.

Our industry is actively contemplating disaster scenarios such as widespread electricity blackouts, marine and aviation collisions, damage to industrial facilities with following business interruption, mass interruption of online services and mass leaks of private information. All scenarios would trigger years of litigation.

A further issue is the lack of consistency in rulings to date. Cyber coverage has been 'found' in traditional lines where underwriters clearly had no intent to provide such protection – if the exposure was not priced for, then the coverage was not expected, and the claim is unanticipated. The rapidly evolving data privacy regulations (and the public concerns that are driving this regulatory activity) add to the uncertainty. Further complicating the landscape are the layers of regulatory activity, whether at the Federal and State levels in the US, or the national and pan-member level in the European Union. Data privacy means different things to different people, and the definitions of what data to protect, how to protect it, and what constitutes a breach is developing rapidly. For international insurers, handling data across national borders adds yet another level of complexity (and exposure for their own operations).

AGGREGATES ARE ESSENTIAL FOR A SMOOTH ROAD AHEAD

As noted, the disaster scenarios are concentrating minds. Not only must cyber risk data be properly collected, and the risk underwritten and priced for, but the exposures must also be carefully tracked for aggregation purposes.

Our industry has spent a lot of time and money understanding the aggregation potential for 'localized' natural events such as earthquake, typhoon and flood. Cyber exposure is man-made, deliberate and global. Consider a situation where several, sizeable financial institutions are subject to a Distributed Denial of Service (DDoS) attack (it has happened already to at least one country).

Our industry is actively contemplating disaster scenarios such as widespread electricity blackouts, marine and aviation collisions, damage to industrial facilities with following business interruption, mass interruption of online services and mass leaks of private information. All scenarios would trigger years of litigation.

Imagine that eight of the 10 banks buy a cyber policy, and that each buys $500 million of limit. Now imagine that one large global insurer participates on four of those eight policies. Very quickly, the reinsurance panel can be exposed to a significant amount of limit. Losses can add up quickly.

Of all lines currently getting the most attention, Business Interruption stands out due to the severity of potential cyber losses: a cyber-attack on an energy utility's infrastructure causes widespread outages. We are now seeing contingent BI/dependent BI more often, yet lack of data makes this difficult to accurately price and underwrite, opening the way to aggressive (i.e. less conservative) assumptions. Contingent BI has the potential to create systemic issues if a major supplier fails: if it must be written then it should only be done on a very limited basis, with low limits and named supplier wording.

Clash scenarios can cause aggregation issues - imagine a cyber-attack causes a large scale breach of data from a retailer. Their sales may be impacted as a result of reputation damage. If this impact is severe enough, it may affect sales targets and the stock price. If the retailer's directors and officers had not done sufficient due diligence to ensure the protection of the customer data, they may face a lawsuit from aggrieved stockholders. Smartly, the retailer had bought both cyber and D&O policies. Both will be impacted, as will the (re)insurer.

TECHNOLOGY WILL CREATE SPEEDBUMPS ON THE ROAD AHEAD

Cyber-attacks are deliberate, global, man-made events that are intended to cause harm: they are the dark side of the rapid technological developments that are positively transforming how we all live and work.

To effectively underwrite cyber exposure, we must all grapple with cybersecurity developments and deployments, the Internet of Things (for e.g. sensor controls), drones and telematics (e.g. remote and artificially intelligent controls). Until recently, tech companies competed on features and capabilities rather than on privacy and security. As a result, many newly deployed technologies are easily hackable - hacks that have the potential to cause physical property damage, as well as **human physical harm.** Medical advances include insulin pumps and pacemakers that rely on sensors to deliver insulin or defibrillators to speed/slow heart rates. As the ability to hack such devices has been demonstrated, the risks have moved beyond Hollywood/science fiction into our real world of insurance exposure. Fiat Chrysler issued Jeep customers with USB devices to update their vehicle's software and strengthen its security features after Wired Magazine demonstrated how to hack the vehicle through its digital radio and manipulate the radio, air conditioning, windshield wipers and transmission.

As consumers understand the trade-offs between convenience and security, we may expect technology companies to pay more attention to cyber defense. However, that change of mindset will take time to filter through to production, until when new technologies must be classified as a potential threat to insurer profitability.

FORTUNE FAVORS THE PREPARED

Society has a clear need for our industry's risk mitigation and risk management skills, and for our keen understanding of the interconnections of cyber-risk exposure across multiple product lines. Preparation and protection improve the resilience of people, businesses and governments to the threat of cyber-attack. More insurers are offering products and services, and more industries are seeking protection. The buyers want higher limits, and wider coverages. Our industry's ecosystem of modeling and other vendor services is flourishing. Rapid, profitable progress will be maintained if we vigilantly heed the caution signs and maintain a well-defined exposure identification and aggregation strategy.

BIG DATA, BIG CHANCES: EFFECTIVELY SECURING TECHNOLOGY, DATA... AND PEOPLE

BY MARK MCLAUGHLIN, IBM

About the Author: Mark McLaughlin is IBM's Global Insurance Director. Mark leads IBM's Global Insurance team, predicting industry business and technology trends, leveraging those insights for the world's largest insurers, and developing IBM solutions in conjunction with our business partners in the insurance vertical. He directs IBM strategic collaborations with senior industry leaders, bringing IBM's experience and innovation together to build sustainable competitive advantage for insurers. He also presents insurance industry research frequently to insurance conference audiences worldwide.

Mark previously has led business units in insurance distribution and analytics, technology infrastructure, CRM, and insurance business process. Mark has personally led implementations in strategy, program management, analytics, data warehousing, expert systems, commercial claims, underwriting for multiple top 20 US insurers. He is a 20+ year veteran of the insurance industry. Mark was a presenter at IRUA's Emerging Risks seminar held in March 2016 in New York City.

Abstract: Almost every insurer these days is talking customer-centricity or digitization, and underpinning those efforts is an interest in Big Data. What do we mean by Big Data? It includes both existing and non-traditional sources of customer, risk, and market information that can be leveraged to find new insights that inform more thoughtful insurer action. Let's explore briefly the possibilities and risks inherent in Big Data, and how insurers and reinsurers might responsibly profit.

WHAT IS BIG DATA

Big Data shares four key attributes that are relevant to insurance decision makers:

- **Volume** – exponentially larger amounts of data as new sources (video, voice records, telematics and the Internet of Things) come on line;
- **Velocity** – generated at speed, often in real time – and requiring interpretation at speed to maximize value of insights gained;
- **Variety** – a wide range of data sources touching all manner of people, objects, and systems; and
- **Veracity** – the data is inherently not precise to the level needed for 100% repeatable results – there is inherent uncertainty. The insurance industry collectively often has trouble with that last point.

Insurers and reinsurers are used to highly structured data and often undertake extensive "data cleansing" to allow for discrete decision-making based on a well-defined set of codes. Big Data implies less certainty – but much greater predictive range, useful for a wide array of risk assessment, sales, and marketing situations.

When people talk about how to leverage Big Data today, what they really mean is leveraging Big Computing – new capabilities in cloud, cognitive systems, and analytics that are revolutionizing which data is available, relevant, and valuable. The promise of this revolution is the ability to build further insight into risk, more finely manage rating and underwriting, and actually take predictive actions to more effectively manage risk. But there are pitfalls in data sufficiency, actuarial repeatability, and security for all firms in the insurance industry data chain.

BIG DATA'S BIG FUTURE

Our ability to interpret data is growing by leaps and bounds. That ability is powered by Moore's Law, which has multiplied calculation power available per $1000 by 1000x over roughly five years. Computing scale has enabled new techniques that sift and analyze all sorts of non-discrete data: Facebook posts, Wikipedia, call center recordings, CNN. We are no longer limited to data that we can house in a designed, cleansed data warehouse.

Such data comprises an increasing percentage of worldwide data, now climbing well over 50%[1] We now can do things like identify interesting events in long video streams, infer human needs from psychographic and social data, and find hidden human relationships – both good and bad – across large pools of identity data. These tools give us new ways to monitor and manage risk.

And we can aim these tools at completely new types of data, available via our vastly increasing connectivity and sensor base. We now can monitor autos and drivers with telematics, see breakdowns occurring in home appliances, and understand worker safety patterns via commercial enterprise monitoring. We can even wire ourselves, and our teams, with wearable data sensors that can do everything from monitoring wellness of the elderly and sick, to noticing when construction workers are having trouble with heatstroke or fatigue. The breadth and detail of available data is unprecedented, but so is that data's ability to describe and define individuals.

USING BIG DATA

The range of Big Data provides new models of insight for a wide range of companies. For insurers, we can identify emerging risks in the marketplace as people ask questions in search engines about mold or identity theft. We can explain those risks in better ways, by choosing explanations that match individuals' emotional

makeup, and providing social data that illustrates how peers are making similar choices. And we can predict specific perils before they occur by detecting preconditions – failing electrical wiring, poor posture when picking up heavy objects, diet changes that are precursors to failing gallbladders.

Those insights also power new modes of risk management and remediation. We can activate systems in response – pumps, brakes, alarms. We can send alerts to insureds to take action to avoid a hailstorm, to caregivers to alert them of an Alzheimer's patient leaving the grounds, and to emergency response personnel to check a potential fire. The insurance agent, too, can be kept in the loop to help guide the insured through a risk situation and offer trusted advice. Big Data systems free humans to focus on trust and relationships, adding more value to the insured experience.

Our options are broadening for advice as well, with the same systems that provide insight to insurers now becoming agile enough to answer questions in spoken language or via a text chat. Cognitive systems can multiply the value of risk insight by giving insureds and prospects a common-sense way to ask questions, get answers, and refer to a human agent when ready.

All of these changes are increasing the underlying value of data, and that data is being kept longer and in more forms. That makes the sheer amount of data in the world staggering - and growing at rates faster than our ability to analyze it. Big Data has become "Ginormous Data!" as my daughter would say. The volume of data is so large that we literally cannot manufacture storage fast enough to store it all. In addition, personal data increasingly has a half-life, with much of it losing value within seconds if not analyzed and acted upon. Summarization, data science, and data strategy are becoming must-have disciplines.

BECOMING BIG DATA DEPENDENT

As companies build their competence in data science, however, this creates personal and professional dependency on data security. Data linked to a person can imply a great deal about personal habits and situation. Many technology users are comfortable today with the tradeoffs of providing personal information, but they are largely unaware of the extent and depth of the data they are providing.

Even anonymous metadata, when paired with other public data, can infer a great deal about where a person works, where they shop, where they worship, which doctors they see, and who they associate with.

So pools of personal data – even ones that seem fairly innocuous – have great value, both obvious and hidden. These issues are already creating regulatory concern, with penalties in place for loss of personal data that are geared to percentage of corporate revenue in some markets. The inferred liability on holding customer data is significant.

BIG DATA RISK

Enter cyber-risk – the risks inherent in a breach of a company's technology regime. Threats have moved well beyond the casual hacker, with organized data theft collectives leveraging myriad vulnerabilities in business technology infrastructure. Data thieves attack network and connectivity, authentication and security regimes, and physical technology plant. And they attack employees as well, using everything from social trust engineering and phishing to active solicitation of employees to commit theft. Big Data has big value, and theft rings can realize millions of dollars from resale of data on open dark-net markets.

Companies of all types therefore face cyber-risk – as long as they keep any information whatsoever about customers or payments. The perils are significant. Company boardrooms in a recent survey cited the following prioritized concerns around cyber-risk[2] :

- Company reputation and brand;
- Lost time and productivity of workforce;
- Cost to remediate data issues for customers;
- Cleanup cost – forensics, hardening of technology infrastructure;
- Notification costs; and
- Legal liability and regulatory penalties.

So what to do? Insurers are responding with cyber-risk coverage, with the market growing 100% per year.[3] Despite significant problems in frequency prediction, very high loss exposure, and limits in reinsurance capacity for the market. To bolster their cyber-risk products, forward-thinking insurers are integrating a wide range of needed technology protections into their cyber-risk coverages.

A wide range of protection is needed. To combat cyber-risk, businesses and IT departments need to address a wide range of security issues:

- identity verification;
- application security;
- data physical security;
- cyber detect/response;

CONTINUED ON PAGE 8

BIG DATA, BIG CHANCES...

CONTINUED FROM PAGE 7

- infrastructure protection;
- threat management;
- leverage of early warning networks (IBM monitors 100m endpoints and has conducted 23 billion URL scans);
- anti-spam to screen phishing; and
- active penetration testing to protect employees;

IT STRESS

Corporate IT departments, however, face a number of pitfalls in combating cyber-risk. One big issue is finding appropriate skills. Increasing technology concerns have created a bidding war for security experts and the value for top experts climbs rapidly. The platform players, like cloud and social network providers, can (and do) afford to hire the best in this environment, leaving a market for skills with significant limitations. In this arena, hiring a bad security practitioner is worse than not hiring one, as it creates a false sense of security that opens vulnerabilities that could have been addressed by proper external support.

Cyber-risk has fostered a number of security services and software firms, many of whom pitch their solution as a be-all/end-all. Given the number of openings for bad actors, strong protections of one or two security holes are not overly helpful. Companies need a holistic approach and assessment of their cyber-security from qualified experts. Insurers are partnering with security firms in part to address this widely understood need.

So companies looking at Big Data really do need to move forward. Insurers face too many obstacles in customer acquisition and retention and in expense control not to leverage every tool they have to connect with end insureds. Insurers need to move to a risk partnership model with their insureds to continue to provide the value and service level those insureds expect. And they need to leverage Big Data to improve their advice, their engagement, and their relevance.

In a world where people check their social media 70 times a day, insurers must up their connectivity game. Insurers who lose their connection to customers risk being relegated to commodity provision of insurance underwriting services in a back-office function, at high competitiveness and low profitability.

FINAL WORDS

A wide range of protection is needed. To combat cyber-risk, businesses and IT departments need to address a wide range of security issues.

Companies need a holistic approach and assessment of their cyber-security from qualified experts.

But with Big Data comes big responsibility. Insurers need to pay attention to their risk assessment in onboarding this data – and use that assessment to make a case for strong cybersecurity measures. There is a wealth of tools and expertise available, offered in conjunction with several insurers as part of cyber-risk policies, as well as standalone. Insurers have too much invested in their brands, their reputation, and their customers not to take advantage.

1 IBM Research, 2015.

2 Ponemon Institute 2015 Data Breach Study.

3 Advisen, Cyber Liability Insurance Market Trends: Survey (Partner Re, October 2015).

CYBER RISK EXPOSURE AS IT CONCERNS DATA AND ACTUARIAL MODELING

BY JOHN FERRARA, ERNST & YOUNG

About the Author: John Ferrara has more than 24 years of experience in the insurance industry. Mr. Ferrara is a Senior Manager for Ernst & Young in its New York office and spends a good part of his time servicing reinsurance clients. Prior to Ernst & Young, he served as the Chief Actuary for QBE, and previously opened a branch agency of Arrowhead General Insurance Agency following his role as Chief Actuary for JLT Re.

Abstract: This article discusses the evolution of cyber breach and cyber risk and identifies the elements of this risk. The author then discusses catastrophe-type modeling for this growing risk and discusses the future of cyber risk modeling.

Cyber breach exposure has been a significant and growing risk for many years. Cyber attacks began in the 1980s. These first attacks focused on breaking into systems because at that time just breaching a system was a challenge.

Over time, these attacks morphed into more sophisticated attacks focused on targeting businesses or entities for financial gain. Breaching a computer network has become a "business" for cyber criminals and hackers. Cybercrime has evolved to include cyber espionage, often perpetrated by current and former employees. Today's cyber breachers include organized crime and even foreign states focused on political objectives.

As a result of these increasing and evolving cyber attacks, cyber loss exposure has become an area of greater interest and concern for the insurance and reinsurance industries. In turn, there is an increasing need to quantify cyber exposure, with an initial focus on what historical loss information is available to the general public and the insurance and reinsurance communities.

COSTS AND CONSEQUENCES

With globalization and an increasingly connected world, the potential for damage and costs of cyber risk are significant. The risk of a cyber attack is multi-faceted, with far-reaching consequences extending beyond the actual data breach. There is reputational risk, loss of confidence and, particularly in the financial and banking sectors, risk of insolvency. In many sectors, cyber risk is now seen as one of an enterprise's most significant business risks.

The industry's regulators have also begun to recognize the significant costs of cyber risk. Violations of the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley Act (Sox) and the Health Information Technology for Economic and Clinical Health (HITECH) Act can easily result in fines, penalties, and worse. Even rating agencies are incorporating the handling of cyber risk into their rating analysis. The impact of these new industry standards will definitely have an important effect on the cost of cyber risks, which can be determined as part of the risk quantification/risk mitigation frameworks, discussed below.

MEASURING THE RISK

A key question central to managing cyber risk is quantification. Quantifying cyber risk exposures will help companies appropriately prepare for and protect against imminent cyber threats. Assigning a quantitative value to cyber risk can be done with risk quantification thus allowing an entity to reduce and mitigate the risk.

Risk quantification is possible today using emerging techniques, including scenario testing, loss distributional models and risk ratings. Risk mitigation strategies today are structured based on cost benefit analyses that fit within an existing and enterprise risk management (ERM) framework. In an ERM framework, cyber risk is usually identified as a major risk, with consistent treatment of the risk throughout the organization. In addition, risk mitigation requires stakeholder communication, both internally (senior management, board of directors) and externally (regulators, rating agencies, analysts and investors). This can include stress tests on the volatility of earnings, as well as being necessary for compliance on publicly traded companies.

Although cyber losses may be identified in typical data reported to rating bureaus and data collection agents for the insurance industry, in general, there is no special data requirement regarding reporting cyber loss data. The most useful cyber data available today is compiled by data collection companies and

CONTINUED ON PAGE 10

CYBER RISK EXPOSURE...

CONTINUED FROM PAGE 9

companies that conduct cyber surveys. The data is collected from press releases and publicly available information, as well as information that companies are willing to disclose by means of a survey. Information technology vendors and governmental agencies that investigate criminal activity and technology issues have noted that this publicly disclosed information is only a small subset of the universe of actual cybercrime activity.

Once it is acknowledged that there is significant cybercrime activity present and therefore a strong need to quantify potential exposure to such activity, it's key is to identify the actual potential loss experienced in the event of a breach in the systems. Oftentimes, companies are aware of a breach but, immediately thereafter, find it difficult to determine exactly what has been stolen and what economic loss, if any, they face. From an insurance perspective, there is no standard insurance policy coverage for cyber exposure. Coverages provided and losses to a company that are generally incurred and may or may not be covered include the following categories:

1. Investigation costs:
    a. Costs to investigate outages or system issues, or to detect unauthorized access; and
    b. Costs to understand breadth of attack and number of systems impacted.
2. Regulatory response:
    a. Legal, technical and forensic service; and
    b. Fines, penalties, regulatory actions and investigations.
3. Lost business:
    a. Short-term – system interruptions, no ability to conduct business;
    b. Retail – less traffic due to adverse news; and
    c. Long-term - lost business due to reputational harm; may be difficult to quantify, but can be significant.
4. IT infrastructure repair:
    a. Consultants and security firms;
    b. Restoring hardware and software costs;
    c. Advice on actions to take after cyber event; and
    d. Litigation preparation.
5. Corporate:
    a. Private financials, trade secrets, communications.
6. Stock losses:
    a. Currently, no clear relationship between cybersecurity attacks and stock price losses.
7. Notification costs:
    a. Notify customers, employees or other victims.
8. Crisis management:
    a. Public relations education on event.
9. Credit monitoring and fraud monitoring:
10. Media liability:
    a. Copyright, trademark or service mark infringement.
11. Privacy liability:
    a. Employees or customers.
12. Cyber extortion:
    a. Employees or customers.
13. Class action lawsuits:
    a. Based on duty to secure personally identifiable information (PII).
14. Bank suits:
    a. Based on loss sustained by banks on credit card breaches.
15. Defensive responses:
    a. Increase money spent on security and new hires: and
    b. Educate workforce on best practices.

Given the uncertainty and lack of significant data, it is difficult to price this insurance coverage and the market appears to have underpriced cyber loss exposure in previous years. Premiums are on the rise; for example, Marsh & McLennan, among others, has cited a rate increase as high as 15% in 2015.

THE CATASTROPHE MODEL FOR CYBER BREACH RISK

A number of industries have unique susceptibilities to cybercrime. Health care records, for instance, offer a high-value per record, as these records can be used to obtain high-value drugs and equipment. Additionally, compromised credit cards are often sold on the black market, but regardless of the particular vulnerabilities, some method must be used to measure and price the cost of mitigating against the risk of a cyber intrusion.

The market has no stable or universal data or means to quantify risk exposure, but there is a need for insurance market capacity for cyber insurance.

There have been several major cyber losses, the majority of which the public is aware of, over the past several years. Some of the major notable events over that timeline include the following:

1. AOL (2005-06)
2. TJ Maxx (2007-08)
3. Heartland and the US Military (2009)
4. Sony (2010)
5. Court Ventures (2011)
6. Massive American business hack (2012)
7. 7-Eleven, JC Penney, Hannaford, Heartland, JetBlue, Dow Jones, Euronet, Visa Jordan, Global Payment, Diners Singapore and Ingenicard (2005-2012; as part of the largest data breach in US history)
8. Evernote, Living Social (2013)
9. The Home Depot, Target (2014)
10. EBay, JP Morgan Chase (2015)
11. Anthem, Ashley Madison (2015)]

Actuaries are aware of cyber loss potential and the lack of related available data. In typical account pricing, actuaries experience rate and exposure rate individual risks. In the case of cyber coverage, actuaries are at a disadvantage for modeling individual accounts since cyber loss is a rapidly evolving exposure with very little complete historical experience.

In addition, no bureau-rating database exists to facilitate industry exposure rating. Once one disregards the numerous small attritional losses associated with cyber breaches, the nature of cyber loss activity is typically low-frequency, high-severity for actual loss activity; so again, experience rating may not be of great value.

The best analogy here may be a property catastrophe modeling approach. Currently, the major catastrophe modeling companies are working on building catastrophe-type models for this exposure. Insurance technology vendors currently have some first-generation models and rating approaches available for cyber exposure. Both BitSight and SecurityScorecard have rating models currently available.

Currently, the major catastrophe modeling companies are working on building catastrophe-type models for this exposure.

The current state of actuarial modeling has certainly improved, as there are now vendor options and data options available as new commercial models are being developed.

In addition, AIR Worldwide and Risk Management Solutions ("RMS') have announced that they are in the process of developing models. Some insurance companies have teamed up with security monitoring and rating companies to provide some form of continual risk management servicing based on company system activity. At best, there is a lot of variability associated with actuarial modeling and there is no universal answer on how to quantify and price cyber exposure. However, although limited, there are models currently available and the actuarial processes related to cyber exposures are improving rapidly.

THE FUTURE OF CYBER RISK MODELING

In summary, cyber insurance and the quantification of cyber risk are evolving and growing. PartnerRe has cited that the cyber insurance market was $1 billion as of October 2014, $2 billion as of October 2015 and is predicted to grow to $4 billion by 2020. The market has no stable or universal data or means to quantify risk exposure, but there is a need for insurance market capacity for cyber insurance. In particular, cyber insurance lends itself to a provision of some form of ongoing risk management service, as this particular exposure is continual and will evolve quickly during a policy period.

The current state of actuarial modeling has certainly improved, as there are now vendor options and data options available as new commercial models are being developed. The additional risk created through correlation among cyber risks for an individual company and an industry sector is not well understood and the true impact of a cyber catastrophe is still difficult to determine. The specific elements of a loss are not well-defined and estimating severity is a challenge. Components of cyber risk, such as reputational risk, which is the largest component of cyber exposure, is often the hardest to quantify. Modeling is also challenging due to an increasing trend that causes cyber data to become quickly outdated. The projection of future costs and whether future costs can continue to escalate at a very high rate becomes highly debatable.

CYBER RISK AND THE EVOLUTION OF SUPPLY CHAINS

BY OLIVER BREW, ASPEN INSURANCE

About the Author: Oliver Brew is Global Head of Cyber Risk & Head of International Professional Liability, Technology Liability & Cyber Risk at Aspen Insurance. Prior to joining Aspen he was Senior Vice President, Head of Errors & Omissions (E&O) with Liberty International Underwriters.

Oliver has more than seventeen years of industry experience.

Abstract: Not only are supply chains becoming more global, complex and integrated, but the liability landscape is also changing as more companies are held responsible for their supply chain delivery. A break in the chain can cause heavy financial losses and management of risk, including cyber. This paper explores emerging trends in global supply chains and cyber risk, outlining strategies businesses can employ to protect themselves and keep the flow of goods and services moving in a world where cyber criminals are constantly evolving their own strategies for launching disruptive attacks.

Global supply chains are a way of life for modern businesses, but in the constant search for affordable labor and services, new challenges and risks have emerged. Businesses must contend with the added complexity of managing production across various locations in different parts of the world, and manage each location's individual risks, from political unrest to natural catastrophes. The 2011 Tohoku, Japan earthquake and tsunami drove home the realization that a single point of failure at a single link can halt the flow of goods across the entire supply chain.

To meet the new challenges, businesses are finding new ways to increase communication and coordination across their supply chains, using technology to integrate systems. At the same time, they are creating redundancies in their supply chains, allowing them to divert production to an alternate location should a supplier be taken offline for any reason.

Amid these trends, cyber-crime lurks with massive financial incentives for criminals and an increasingly connected world on which to launch attacks. Some supply chain trends play into the hands of those who perpetrate cyber-attack. For example, efforts to integrate supply chains by connecting systems and getting them to talk to one another create opportunities for cyber criminals to infiltrate systems throughout the chain by infiltrating the weakest link. However, some of the tactics businesses are using to manage supply chain risks can also be used to manage cyber risk across the supply chain.

Essentially, a failure at a single point in the supply chain can cause a bottleneck that slows or halts the ongoing flow of goods.

Companies that make serious efforts to audit their supply chains to better understand risks can also assess their suppliers' and vendors' cyber security efforts. And the trend toward creating redundancy in supply chains can help businesses should a cyber-attack take down a supplier.

THE EVOLUTION OF SUPPLY CHAINS

Supply chain development is proceeding along three dimensions:

- Supply chains are becoming more global and complex — The outsourcing era continues as companies identify new affordable places to produce their products.
- Supply chains are becoming more integrated — To fight increasing complexity, companies along supply chains are leveraging technology to collaborate and better coordinate their decisions.
- Supply chain optimization — Companies are trying to optimize their production, inventory, and logistical decisions along the chain, bringing the concepts of lean production and six sigma to supply chains.

Dr. Fangruo Chen, MUTB Professor of International Business

at Columbia Business School's Decision, Risk, and Operations Division, explains, "If you think about supply chain evolution, or innovation, in the past few decades, think of it in terms of the scope being more global and more complex, the relationship between members of the supply chain becoming more integrated or more cooperative, and, finally, companies improving the quality of decisions through optimization and identifying technology solutions and strategies that help them effectively manage and make decisions across the supply chain."

SUPPLY CHAIN RISKS

The evolution of supply chain development has brought with it an evolution of risks. Because supply chains have become so extended, a problem at any link in the chain can cause a major disruption for multiple parties. Essentially, a failure at a single point in the supply chain can cause a bottleneck that slows or halts the ongoing flow of goods.

Potential risks come from many directions, such as natural catastrophes which can disrupt suppliers and cause capacity issues, notably seen in the aftermath of 2011's Tohoku, Japan earthquake and tsunami [1], and, more recently, when earthquakes struck the south of Japan [2] in April 2016.

This risk is not limited to the physical production of a good: a company may be dependent on a vendor for payroll, security services, or benefits. An outage at any of these suppliers could cause a significant knock-on impact for the company relying on the service. Other risks abound. Political risk around the globe could halt the flow of goods along a supply chain, as could the failure of a machine at a supplier's factory.

Beyond the flow of goods, the quality of products can be compromised at any point along a supply chain, from the raw materials to the semi-finished product. A recent, prominent example is the massive recall [3] of all Takata-made ammonium nitrate-based driver and passenger airbags that do not use a drying agent, affecting a wide range of car makes and models across a number of model years.

The complexity of supply chains has also changed the liability landscape. A company may be ultimately liable for quality issues that occurred at a supplier. "This is a changing environment, and it seems like it's more and more true that companies will be responsible for what their supply chain is delivering," Dr. Chen says. "It's not just what you do, but what your upstream suppliers do." Dr. Chen also points to "invisible risks" in supply chains that companies have to anticipate, which gets complicated when real money has to be spent to try to prevent them. "Potential is hard to quantify," Dr. Chen summarizes.

COMBATING SUPPLY CHAIN RISKS

Companies have adapted to the changing environment through supply chain risk management — where risks to the supply chain are constantly assessed and strategies are developed to manage them.

Steps include:

- Audit programs — Companies are making a continuous effort to get more information about what is going on along their supply chains, and they are taking proactive steps before disruptions occur. This includes company executives visiting and inspecting production sites, with Apple CEO Tim Cook visiting Foxconn's manufacturing plant [4] in China being one well-known example.
- New supply chain design — Companies are looking at making supply chains more robust and able to deal with global risks. For example, diverting production should a problem occur at one link in the chain. As Dr. Chen notes, this is "easy to say, but very hard to do."

WHERE CYBER RISK FITS IN

It's hard to avoid the topic of cyber-risk today. It is a threat to businesses of all kinds, even in sectors far removed from retail, banking, and health care, where breaches have been well publicized.

Attacks come in many forms, and the motives behind them are clear: in today's world, there is money to be made in stolen data, and lots of it. Statements last year [5] by SEC Commissioner Luis A. Aguilar indicate the market for stolen credit card data alone is $114 billion. Add in the value of other types of data, such as medical information, and even company trade secrets, and it is easy to see why cyber-attacks are carried out.

Cyber-attacks can also be politically motivated or perpetrated by activists. As long as these motives remain, criminals will continue to carry out cyber-crimes. And as our world continues to rely so heavily on computers and networks, with advancements such as the Internet of Things promising even closer connectivity, criminals will innovate and find new ways to launch attacks.

The good news is awareness among businesses is increasing and companies are taking the threat more seriously than ever. Whereas cyber may have been seen as an IT risk historically, it is now generally recognized as an ERM challenge, with the conversation about how to address it elevated to include a company's top executives. In other words, it is becoming clear that cyber risk is a business risk.

CYBER RISK AND SUPPLY CHAINS

For a business, recognizing cyber risk within its four walls is one thing, but organizations must also understand this risk in the context of their supply chains — whether they rely on suppliers spread across the globe to manufacture products, or whether they use IT services from a cloud provider. As some have unfortunately discovered, companies can in fact be impacted by a cyber breach along their supply chains.

In the 2013 Target cyber breach, for example, attackers got into the system [6] with credentials stolen from an unlikely third-party vendor: an HVAC subcontractor. A cyber breach along a supply chain can take a number of forms, and affect a company in a number of ways. These varied threats correspond to the major themes discussed previously regarding supply chain trends and risks:

- Supply chains are becoming more global and more complex, and, as discussed, since they have become so extended, an

CONTINUED ON PAGE 14

CYBER RISK AND THE EVOLUTION OF SUPPLY CHAINS, CONTINUED FROM PAGE 13

event such as an earthquake or major storm suffered at any link in the chain can disrupt the flow of goods or services. The issue, though, does not have to be a natural catastrophe. If a supplier is taken offline by a cyber breach, the net effect is the same.

An attack may not be limited to a supplier's systems, either. A more recent trend shows cyber-attacks can cause physical damage at facilities. Reports in January 2015 revealed a steel mill in Germany suffered "massive" damage [7] when a cyber-attack disrupted the control system to a blast furnace, preventing it from being properly shut down.

- Supply chains are becoming more integrated, which carries both benefits and risks. On the one side, a more integrated supply chain can enable real time communication and efficiencies. On the other side, if systems and networks are more open, then they're more vulnerable.

The danger is that if multiple parties throughout the chain are networked, then, as in the Target breach, attackers can use a supplier or vendor as the point of entry into a company's system. Dr. Chen says many businesses are only beginning to recognize this threat, as the priority has been accomplishing the difficult task of getting systems across the supply chain to talk to one another. "The risk is a fairly recent realization," he says.

- The liability landscape is being reshaped by supply chains — as noted, a company could be liable for a defect that originated at one of its suppliers. This is just as relevant for data as it is for products and services. John Mullen, Partner/Chair of the U.S. Data Privacy & Network Security Group at Lewis, Brisbois, Bisgaard & Smith, LLP, explains that the company initially entrusted with customers' data is generally seen as the data owner for purposes of liability and legal duty. This means that while the data may have been passed on to and compromised at a supplier, the initial holder, with some exceptions, will have to respond to a breach.

Even as businesses take steps to address cyber risks and supply chain risks individually, connecting the dots to identify and address cyber risks within their supply chain is not yet as widespread as it should be.

Dr. Chen says news stories about cyber breaches along supply chains catch attention, but as far as prioritizing supply chain cyber risk, he notes, "My sense is it's not very high on the list." The danger in this outlook, as Dr. Chen points out, is that addressing cyber risk requires constant vigilance. "It's not like a natural catastrophe such as an earthquake," he says. "With cyber, you have an enemy on the other side who is constantly improving." Dr. Chen explains that if businesses are not likewise improving as the enemy gets stronger their vulnerability becomes greater.

EXAMPLES OF CYBER BREACHES

ORGANIZATION IMPACTED: TARGET

When: December 2013

Information compromised: 11 gigabytes of data, including names, addresses, phone numbers, email addresses, and payment card information for up to 70 million people.[8]

Key points:

- Successful phishing attack on HVAC vendor.
- Misconfigured systems enabled effective reconnaissance.
- Network segmentation was lacking so that attackers could pivot to point of sale once inside.

ORGANIZATION IMPACTED: OFFICE OF PERSONNEL MANAGEMENT

When: April, June 2014

Information compromised: Birth dates, addresses, and Social Security Numbers of 4.2 million current and former government employees in breach discovered in April; Social Security Numbers of 21.5 million people and 5.6 million records containing fingerprints in breach discovered in June [9]. Key points:

- The very large cache of sensitive data in non-segmented data base created a rich target.
- Appears from first assessment that subcontractor not involved.
- Likely Chinese in origin but hard to measure motive.

ORGANIZATION IMPACTED: RSA SECURITY

When: March 2011

Information compromised: Computer security products used by corporations and governments [10]

Key points:

- Combination of phishing and advanced persistent threat signifies the importance of people, not just technology, defense.
- The detection defenses worked, but took time to take effect.

PREPAREDNESS AND PROTECTION

Protecting and preparing one's organization is challenging enough. Thinking about the potential vulnerabilities along an entire supply chain can seem daunting. Nevertheless, there are steps organizations can take to begin to understand what they do not understand, particularly with respect to sensitive data within the organization and across its supply chain:

- Know the business — Many companies do not know what data they hold, where it is stored, who has access to it, or when it is purged, says Mullen. Some companies unnecessarily hold on to old client information or other data that is of little use to them, but may be of value to attackers. Mullen advises: "Know your own business. Know where your data is; where you duplicated it; who has access internally and externally — just get a holistic appreciation of where your data sits, moves, and resides." From there, the process of evaluating how to manage challenges can begin.

- Protect the company — Cyber liability insurance is readily available from a number of reputable insurers. While insurance will not prevent a cyber-attack, it will help a company recover more quickly in the event of a data breach or network security failure. The key is for companies to consider their insurance needs in the context of the previous step — they must know what they have before they know what to protect.

A company may believe it is storing 3,000 records, for example, but learns, upon doing an assessment, it has 3 million records. In that case, the company will need more coverage than originally anticipated. "Get your own ship in order and get enough insurance in place to manage any kind of breach you might face," Mullen advises.

Insurance can cover costs associated with responding to a breach, including investigation, notification, and legal costs. Company executives should speak with an insurance professional regarding what is covered and what is not, and to determine the appropriate coverages. When considering supply chain risk in general, company insurance buyers should ask about insurance coverages such as contingent business interruption, which covers costs associated with a property loss at a supplier's location.

Corporate insurance buyers should also:

- Identify the supply chain — Businesses should understand that their vendors and suppliers may themselves use subcontractors. The first step toward managing cyber risk in a supply chain is properly identifying the vendors and suppliers within it and knowing who exactly is handling data and how. Sarah Stephens, Head of Cyber, Technology, and Media E&O at JLT Specialty, says creating a system to keep track of vendors is among the first steps a company should take to manage its cyber risk exposure. "You'd be surprised how many companies can't tell you who their vendors are," Stephens says.
- Set standards and manage network access —Businesses should create cyber security standards for partners within the supply chain that will be handling data — are suppliers at least the company's equal when it comes to security? Sometimes a company may discover a supplier has more stringent standards than its own — some cloud providers, for example, are as successful as they are because they are more secure and robust than the companies that use their services.

Lauri Floresca, Senior Vice President & Partner at Woodruff-Sawyer & Co., notes that, beyond who holds or manages data, companies should consider which vendors have access to their networks. In some cases, it may be a vendor that should not be expected to be on the cutting edge of cyber security.

Floresca notes that the HVAC vendor in the Target breach, for example, would not be expected to have security resources against an attack. Floresca recommends cordoning off and limiting network access to only what each vendor specifically needs.

• Negotiate contracts — To the extent it can, a company should negotiate favorable terms in its contracts with vendors and suppliers. This may be limited by the leverage the company has. A small company using a service from one of the largest cloud providers, for example, will not have much leverage. "But," says Stephens, "where it's more equal, get the best indemnification provisions you can." Adds Mullen, "If you have power and leverage, you can do audits and have protections in contracts, and be in better shape than most." He says the initial contract between the data owner and the first company in the chain is the most important.

If a company has leverage, it can try to put some of the onus on that first vendor in the event of a breach. Stephens recommends requiring small vendors to carry cyber liability insurance. Beyond the actual coverage protections, she says the underwriting process is usually thorough and sophisticated, and can act almost as a second audit beyond the company's own due diligence when vetting that vendor.

Just as cyber supply chain risks were correlated earlier to broader supply chain trends and risks, the above steps for preparedness and protection can be correlated to the strategies businesses are using to combat broader supply chain risks. Think of identifying and assessing cyber risks associated with vendors and suppliers as the audit programs, where companies gather information about their supply chains and take proactive steps to prevent disruptions. And think of cyber liability insurance and contract terms as a company's way of making its supply chain more robust and able to deal with cyber risks.

When it comes to assessing a company's supply chain what is clear, especially for larger organizations, is that it's near impossible to overturn every stone and look under the hood of every organization you interact with in detail enough to get comfortable with their cyber risk. Since it is not realistic to thoroughly audit every single supplier, companies can stick to consistent principles and identify processes, protocols, and systems to manage weak links. Floresca says the goal is for a company to understand what rights it has, and to establish clear expectations about obligations in the event of a breach at a vendor: "How they notify you, how you deal with notifying end customers — do you notify or do they? And who pays for that? What audit rights do you have to go into their network and determine what was breached?"

INFORMATION SHARING AND THREAT INTELLIGENCE

Beyond the basic steps companies should take to understand their own organizations, their supply chains, and their respective responsibilities when it comes to data security and breach response, there is a wealth of available information on specific threats that companies can leverage, if they can separate the actionable information from data that cannot be acted on.

Firms such as FireEye offer services to provide companies with threat intelligence — meaningful data on specific cyber threats that are happening in a given industry. The trick is there can be so many data points and not enough resources within an organization to interpret and act on them — this is a lesson one can take from the Target breach, as Target employed FireEye as a threat intelligence source. Obtaining the data is only an effective strategy if a company is able to properly interpret and leverage it.

Stephens separates companies using threat intelligence into three categories: At the lower end are organizations that receive threat intelligence data from a single source. At the higher end, organizations have a dedicated security operation center monitoring real time attacks and cataloging what they see. They then draw lessons they can specifically apply and look at data sources of third party attacks to gain a fuller picture. Finally, there are organizations that go a step further and look not just at what threats are happening, but anticipate what will happen in the future and examine ways to prepare. Ultimately, companies must make use of what they can, given the resources they have.

As a starting point, Floresca recommends that companies work to identify different potential threats and the likely sources of those threats given their specific industry and business, the data they are holding, and their reliance on networks to operate their business.

She says companies should ask: "Are threats going to be financially motivated, politically be motivated, or carried out by activists? That varies depending on your industry, how visible you are, and what type of information you're holding."

CONTINUED ON PAGE 16

CYBER RISK AND THE EVOLUTION OF SUPPLY CHAINS, CONTINUED FROM PAGE 15

Floresca further suggests companies specifically consider:

- What they need on a day-to-day basis to run their business;
- How revenue will be impacted if networks are unavailable;
- The extent to which operations can be shifted offline if someone is persistently attacking; whether the network runs a manufacturing facility;
- What the worst case scenario is that people within the organization can think of, and how the company can recover.

After examining their own business broadly, companies can then get more specific intelligence from expert sources. Keep in mind: information and actionable intelligence are different, and companies must be able to identify the few pieces of information that will actually improve outcomes.

Stephens recommends companies make smart decisions about what security operations they can insource and what they should outsource, keeping in mind how they can bake security into their outsourcing decisions. "In some cases, for smaller entities, it might be better to rely completely on a managed security provider to manage IT infrastructure, or move basic business processes to a trusted cloud provider," she says.

Larger organizations with better resources and large security teams might do better to insource such operations so they can do a more customized job. Once a company understands and can leverage threat intelligence, it may consider sharing relevant information among its suppliers and vendors. The challenge is sharing meaningful and actionable intelligence rather than all information that passes through systems. Stephens recommends requiring small vendors to carry appropriate insurance, which for some will be technology professional liability with a cyber component, and for some will be cyber liability insurance.

As Stephens notes, the company is not a managed security provider for its vendors, so it should consider when and how to appropriately share information. Hiring vendors that have effective security capabilities is ideal, but for a subset of vendors with useful services but limited security resources, periodically sending an email advising them about a threat to look out for may be an information sharing strategy companies could employ. As Stephens notes, a buyer of services is not a managed security provider for its vendors, so it should consider when and how to appropriately share information. Hiring vendors that have effective security capabilities is ideal, but for a subset of vendors with useful services but limited security resources, steps like periodically sending an email advising them about a pertinent security threat may be prudent.

COMMON MISSTEPS

Mullen offers common mistakes he has seen that companies should avoid:

- Companies should not assume because they have a contract that they are protected in the event of a cyber breach.
- Companies should not assume that because a breach is not their fault that it is not their responsibility. "'Not your fault' and 'not your responsibility' are two different things," Mullen says.
- Companies should not try to manage an event — whether the fault lies with them or with a subcontractor — without expert opinion.
- Companies should make sure they use the right experts in the appropriate role. "I see this a lot," Mullen says. "Companies use 'Company X' to support them for security and IT and bring that exact company in for forensics to fix a problem. What if it was their fault?"

REALISTIC GOALS

It is not possible to eliminate cyber risk entirely throughout a global supply chain. Taking steps to limit risk should not be misinterpreted as an airtight defense against threats. But understanding your organization's operations, its supply chain, and its vulnerabilities can lead to the next best thing: resilience, or avoiding the potential for a single point of failure to disrupt your entire supply chain.

Take the first step, if you haven't already, and take measures to understand your operation and your supply chain. Assemble key personnel within your organization to identify how much and what kind of data you are holding and where it sits. Audit your supply chain to the extent you can and protect yourself as thoroughly as possible through your contracts with suppliers and vendors. Speak with your agent or broker about the proper coverages to help protect yourself against cyber threats and other supply chain risks.

The goal is to do all you can to recognizing threats, limit your exposure, and ensure supply chain redundancy.

---

[1] Stress Test for the Global Supply Chain - The New York Times, March 2011 http://www.nytimes.com/2011/03/20/ business/20supply.html?pagewanted=all&_r=1

[2] Toyota, Other Major Japanese Firms Hit by Quake Damage, Supply Disruptions - Reuters, April 2016 http://www.reuters.com/article/us-japan-quake-toyota-idUSKCN0XE08O

[3] All Takata-Made Airbags Without Drying Agent to be Recalled Through 2019 - Autoweek, May 2016 http://autoweek.com/article/recalls/nhtsa-adds-35-40-million-takata-inflators-largest-recall-us-history#ixzz4APz3Vo5x

[4] Apple's Tim Cook Visits Foxconn iPhone Plant in China - Bloomberg, March 2012 http://www.bloomberg.com/news/ articles/2012-03-29/apple-says-cook-visited-new-foxconn-plant-inzhengzhou-china

[5] A Threefold Cord — Working Together to Meet the Pervasive Challenge of Cyber-Crime - U.S. Securities and Exchange Commission, June 2015 https://www.sec.gov/news/speech/threefold-cord-challenge-of-cyber-crime.html

[6] Target Hackers Broke in Via HVAC Company - Krebs on Security, February 2014 http://krebsonsecurity.com/2014/02/target-hackersbroke-in-via-hvac-company/

[7] A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever - Wired, January 2015 https://www.wired. com/2015/01/german-steel-mill-hack-destruction/

[8] The Target Breach, Two Years Later - ZDNet, November 2015 http://www.zdnet.com/article/the-target-breach-two-years-later/

[9] What to do if you are affected by the OPM data breach - The Washington Post, December 2015 https://www.washingtonpost.com/business/get-there/what-to-do-if-you-are-affected-by-the-opm-data-breach/2015/12/09/534455e0-9dd0-11e5-a3c5-c77f2cc5a43c_story.html

[10] SecurID Company Suffers a Breach of Data Security - The New York Times, March 2011 http://www.nytimes.com/2011/03/18/technology/18secure.html?version=meter+at+1&module=meter-Links&pgtype=Blogs&contentId=&mediaId=&referrer=https%3A%2F%2Fwww.google.com%2F&priority=true&action=click&contentCollection=meter-links-click

Journal of Reinsurance

ADVERTISING INFORMATION

The Intermediaries & Reinsurance Underwriters Association is pleased to announce the sale of advertisements in the Journal of Reinsurance, please respond promptly if you have an interest in reserving space.

ABOUT THE JOURNAL OF REINSURANCE

The Journal of Reinsurance is an official publication of the Intermediaries & Reinsurance Underwriters Association. It is published up to four times per year. Focused on issues confronting the reinsurance community in today's complex environment, the Journal of Reinsurance applies the best research and practices to the strategic challenges and operating problems of today's environment. The Journal of Reinsurance is designed to keep reinsurance and insurance underwriters, insurance company executives, brokers, regulators, academicians and those interested in reinsurance abreast of developments which will impact on reinsurers and the reinsurance market.

For additional information, including ad rates please call the IRUA Member Service Center at 718-892-0228 or email mcs@irua.com.

The Intermediaries & Reinsurance Underwriters Association

In 1967, executives from seven Midwestern insurance companies met in Milwaukee to discuss reinsurance concerns. From that first meeting, the IRUA has grown to become an organization comprised of approximately 35 member companies and firms engaged in the assumption, placement, purchase or management of property/casualty reinsurance.

In October 1993, the IRUA expanded its membership to include reinsurance intermediaries in addition to its broad spectrum of professional reinsurers and assumed reinsurance departments of multiple line carriers. Approximately 25% of the IRUA's current membership is comprised of intermediaries.

In September 2002, the IRUA further expanded its membership to include reinsurance ceded operations of primary insurance companies. While all IRUA members operate principally in the U.S. reinsurance market, several are located in Bermuda and Europe and many are also active in international markets.

In April 2014, the members agreed to expand Affiliate Membership to include providers of services to the reinsurance community such as attorneys, accountants, consultants and financial advisors.

The IRUA is a not-for-profit corporation, organized for the purposes of reinsurance education and research, and the dissemination of information relevant to the reinsurance industry. The IRUA does not speak on behalf of its membership on industry issues nor does it engage in lobbying. To learn more about IRUA visit our website at www.irua.com.

Commentary or Corrections?

The IRUA welcomes your comments and suggestions, as well as information regarding errors or omissions that call for correction.

Please send your electronic message to mcs@irua.com or by telephone at 718-892-0228.

SAVE THE DATE

April 5 - 7, 2017

IRUA

2017 Spring Conference
Celebrating the IRUA's
50th Annual Meeting & Conference

"BridgeTo The Future"

Topics:

- Presentation by Lemonade
- Leading Millennial and Seasoned Veterans Panel
- CEO Roundtable
- Fallout from Brexit
- The Future of Reinsurance from a Reinsurer's Perspective

Among others…

PGA National

400 AVENUE OF THE CHAMPIONS / PALM BEACH GARDENS, FL 33418

Group Rate: $259 (Plus applicable Taxes)

Cut-Off Date for Group Date: March 6, 2017

For Room Reservations Call: 844-821-0028