JOURNAL OF TERRORISM & CYBER INSURANCE

The Journal Of Terrorism & Cyber Insurance

www.terrorismcyberinsurance.com

team@terrorismcyberinsurance.com

March 2018

WELCOME

The team at the Journal of Terrorism & Cyber Insurance are proud to bring you the fifth edition of the Journal of Terrorism and Cyber Insurance.

This fifth edition continues from our earlier editions of the Journal where we featured comments, trends, advice and expert opinions from key global insurance industry professionals, counter terrorism experts and cyber security professionals on the state of the terrorism and cyber insurance market and likely challenges.

We thank you for reading and hope you enjoy all of the contents, articles and features in this edition.

JTCI ONLINE

We welcome followers and subscribers on all our online presences. We also encourage readers to sign up to our email list (website, right hand column, or email team@ terrorismcyberinsurance.com).


team@TerrorismCyberInsurance.com


www.TerrorismCyberInsurance.com


ww.Twitter.com/TerrorCyberIns


www.linkedin.com/company/journal-terrorism-cyber-insurance

Table of Contents

Introduction

This quarter has been a very active one when it comes to man made events be it cyber, terrorism and even the first fatality caused by an automated vehicle. In short and in the context of insurability, there is an increasing trend of events which were caused by man made mechanisms.

Cyber and Insurability of the Evolving Cyber Threats

In the context of cyber there has been no real slowdown in the number or type of attacks. In terms of the trend of attacks there were a consistent and escalating number of attacks which resulted in data breaches. In November 2017, it was reported that Uber had paid hackers to delete stolen personal data of 57 million customers and drivers (including details such as phone numbers, email addresses, names and license plates). There was also a continuation of the trend towards the utilization and exploitation of malware and/ or ransomwear as a means of cyber criminals and cyber attackers seeking to cash in on their skills.

In January 2018, in Japan there was a cyber heist where a Japanese- based crypto currency exchange lost in excess of $530 million. It is believed that this cyber heist was the largest crypto currency heist to date.

There has also been increased fears of cyber attacks which may be targeted in the future at critical national infrastructure or cyber attacks which manifest in physical property or other losses or damage. In October of 2017, there were widespread reports of media outlets, train stations, airports and government agencies within Russia being significantly affected by Malware which was believed to behave in a similar way to NotPetya.

As the number of cyber events increase or the reporting of these events has much more public exposure, there is an ongoing debate over the perpetrators. Recently, there has been a greater discussion of state sponsored cyber attacks. This is a new trend or phenomenon as previously cyber attacks had not been publicly attributed to state actors.

Conversely, as a means of ensuring greater resilience there is an increasing spotlight on the issue of cyber security where companies are starting to consider the issue much more seriously. This is particularly the case as cyber is moving from being perceived as an IT issue to a greater business related issue which is the responsibility of everyone in a company and which should also be a

matter for consideration by the Board of a company. The Board in turn should be guided by knowledge, information and options from Chief Information Security Officers or other skilled individuals within companies or other expert vendors who understand the existing threats, vulnerabilities and options for dealing with these. In parallel to this enhanced publicity of the need for greater cyber there have been an increasing number of initiatives which are designed at educating school children and university attendees about the benefits of becoming involved in cyber. This is not only useful in creating a future frontline against cyber threats as they transform and change but is also provides an outlet and an opportunity for those who at a young age are gifted with computer and technology to employ those skills to help protect people, companies and communities.

The insurance industry has started a much broader engagement in cyber affecting business as a whole and how to think about the issues of cyber. During this period, as one potential means of resolving some of the pressure of cyber and obtaining sufficient capital to help satisfy demands for increasing limits, there was the launch of the first cyber ILW. This ILW is a unique product previously unseen in the cyber insurance market and has occurred in part due to the availability of an industry catastrophic loss index for cyber events.

Terrorism

In the context of terrorism, the events have affected the USA, Russia and most recently France. The tactics which were broadly used during these events have continued to evolve from the more traditional forms of attack using bombs and guns.

In New York, the incident in New York was a continuation of many other events in 2017 which deployed the use of a truck or other vehicle as a means of carrying out an attack and maximizing the number of fatalities. On 31 October 2017, a truck was driven into a bike path in New York which killed 8 people and injured a further 11. Documents which linked the driver to ISIS were found within the vehicle.

In Russia, just after Christmas on 27th of December 2017, a homemade bomb exploded in a supermarket in St. Petersburg. The explosion resulted in injuries to 18 people. In the aftermath of the event ISIS proclaimed responsibility. Similarly, within Russia on 18 February 2018, as churchgoers were existing a church in Dagestan, they were greeted with a reign of fire. This resulted in the death of five

people and it further injured several others. The event coincided with a Christian holiday and the Islamic state claimed responsibility for the attack.

The most recent event occurred on 23rd March and thus as this Journal is being published full details of the event are still emerging. During this event a gunman took a number of hostages in a local supermarket in Trebes in the south of France. There were a number of fatalities and injuries arising from the event. Although it is too early for a formal declaration to be made about whether the event can be categorized as terrorism, to date ISIS have proclaimed they are responsible.

In looking at these events as a whole, the attacks are illustrative of a continued trend of attacks deployed with simple and easy to access devices such as trucks and homemade bombs. The threat of terrorism and the number of attacks, particularly given the trend towards attacks utilizing attack vectors which are easily obtainable (guns, vehicles, homemade bombs etc.) is likely to escalate. It is believed that there is an increase in mechanisms for widespread training with the intent of radicalizing those who can then serve the objectives of ISIS. Although the techniques deployed to date have largely utilized attacks involving easily obtainable items, it is probable that there will be an increase a move towards attacks which deploy various forms of technology for the attack vector in the future.

Although there has been a number of attacks which have carried out to fruition, there have been additional foiled plots. The discovery of terrorist plots and the prevention of such attacks from occurring is due to the diligence of police, intelligence, community and business participation and sharing of information resulted in attacks being foiled. One of these attacks was the plans which ISIS purportedly had to blow up an airplane leaving from Sydney. The foiled plot was to involve a device which would be hidden inside a meat mincer which the attacker was to carry onto a plane. Intelligence surrounding the purported plans have prevented any such attack from occurring. In Europe, there were a number of attacks which were also foiled including the French security forces who reportedly foiled two planned attacks in 2018, where one perpetrator already had bomb-making equipment. Similar attacks have been foiled within the UK and elsewhere in Europe over the last few months.

In addition to Islamist terrorism,

there has been also a growing concern regarding far-right terrorism. In the UK, in the past year at least four specific far right-wing attacks have been foiled. The plots which were foiled, included an attack which was planned to occur at a gay pride march where the perpetrator should the attack have taken place would have used a machete to generate as much damage as possible. From an insurance perspective, the concern is about terrorist attacks and potential loss of life, injury, property and interruption to businesses. Mark Rowley, Head of Counter-Terrorism policing in the UK suggests that far-right extremists are "working in a similar way to Islamist extremists", by creating a distrust of state institutions and increasing intolerance.

Other Forms of Technology

In March 2018, man made technology was in the headlines due to the first fatality caused by an autonomous vehicle. The pedestrian was killed whilst the Uber funded autonomous vehicle was on a test run. From the viewpoint of insurers, this provides a challenge that as technology increases and changes it is important to also ensure or be aware of the limits of technology and new challenges which any advancements may pose. The challenges to insurability can be from the intended uses of a product which is reliant upon technology or from unintended or malicious uses of the same technology.

To date, thankfully there has not been any attacks through the use of drones, automated vehicles or the likes. However, in January 2018, there was a purported attack by 13 armed drones. During this event, the drones were shot down before causing any damage. Although in this case the attack was stopped, it is an example of the evolving challenges and potential future attacks we may be facing. There is growing concern that the Artificial Intelligence systems or drones or automated vehicles may be employed to a much greater extent in the future and as such they may be easy to manipulate, and in doing so generate injury, death or other forms of damage.

This Edition

To reflect the changing nature of cyber risks, a consistent threat of terrorism and challenges and opportunities brought about by other forms of technology, this edition of the Journal of Terrorism and Cyber Insurance provides a variety of content on all of the issues discussed.

IN BRIEF: COMMENTARY FROM THE INDUSTRY

The maritime industry over the last two decades has seen major developments in safety and efficiency. This period has also seen increasing larger vessels being built and a greater reliance on technology. Although these changes have undoubtedly been beneficial to the maritime industry and by extension world trade it has not been without challenges.

In the 21st century maritime industry, the most significant threat is a cyber attack with a blind attack on a mega container vessel in a busy shipping lane such as the Straits of Malacca and the potential consequences of such an attack. Many of the functions of the modern vessel are computerized with navigation systems relying on global positioning systems (GPS) so the threats of hacking and malware as examples cannot be underestimated.

The maritime industry and marine insurance industry have been conjoined for many centuries with the development of maritime industry have a dependence of the marine insurance to insure ship owners and other tiers of the maritime industry for the liabilities they incur. In the modern era this has been a tripartite arrangement with the maritime nations. The maritime industry, its insurers and maritime nations has agreed a framework of international legislation (conventions) whereby ship owners are able to limit their liabilities in the event of certain types of incidents for example pollution and removal of wreck. By extension this has enabled the marine insurance industry to provide insurance coverage at a reasonable cost.

The potential insured liability loss from a cyber incident could dwarf by a major multiple any liability loss that the marine insurance industry has paid to date. The threat of a major cyber attack on the maritime industry is not mere paranoia but regrettably increasingly inevitable.

"The chance of anything coming from Mars was a million to one they said but still they came" – Jeff Wayne's War of the Worlds

Laurence Winter, Head of Marine Liability, AmTrust

IN BRIEF: COMMENTARY FROM THE INDUSTRY

Terrorism is constantly evolving and unfortunately the tactics are becoming more diverse. Merely focusing on the last attack will not necessarily protect you from the next. The attack in Barcelona marked a move towards vehicle borne explosives attacks. This style of attack is deadly and it doesn't take too much imagination to think of the results of a large vehicle bomb crashing into a building full of people. But of course the tactics are decided by the terrorists. Our role is to reduce our vulnerability. Businesses should be ensuring that they take care of their staff and give them as much help and training as possible to stay safe. This is especially the case if they are located in cities or you are asking them to travel for business. After so many attacks, no business will be able to use the excuse that they were were not aware of the high terrorism threat levels.

Chris Phillips GCGI FSyl FCiiSCM, Managing Director, IPPSO Limited

IN BRIEF: COMMENTARY FROM THE INDUSTRY

As we all know, capacity breeds experience and a first step towards expanded capacity has been achieved through the introduction of the first cyber ILW product. The benefit of the ILW is that the market loss or index will be determined independently and from an objective decision-maker who can determine the size of a market loss. This will give cyber underwriters the perfect hedging mechanism to start realizing the potential of the cyber market while still improving and developing a more mature market for it.

Alex Mican, Senior Product Development Manager, PCS

Language of Jihadism

Summary

The military defeat of ISIS did not eradicate jihadism and jihadi networks worldwide. Their activities are likely to continue and draw new recruits and supporters. This article suggests looking at the often ignored reason of the continuity of jihadi appeal since the end of the last century, namely the principles and methods of the language they use. Despite the evolution of jihadi warfare tactics, their language operates according to the same principles. Their linguistic methodology can be summarized as "pro-war populism", which is aimed at triggering emotional reactions and provoking participation in terrorist activities. Until governments find a widely acceptable solution on how Islam should be incorporated into the state fabric, jihadi language will have its consistent audience. Meanwhile, counter-terrorism and risk management experts should engage with jihadi messages and expose their linguistic methods for people to be able to recognize and resist them.

ISIS and continuity of jihadism

In December 2017 Iraqi Prime Minister Haider al-Abadi declared the end of the three-year war against ISIS. Around the same time, UK Foreign Secretary Boris Johnson delivered a speech on the British foreign counter-terrorism policy. Voicing congratulations on the success against the so-called Islamic State, he still cautioned against over-confident jubilation: if the group was defeated, their ideology remained alive.

The so-called Islamic State group managed to draw world media attention in 2014 after capturing territories in Iraq and Syria. The movement grew out of jihadi training camps in the Afghanistan-Pakistan area established in 1999 by Jordanian jihadist Abu Musab al-Zarqawi. He fought against invasions of Afghanistan both by the Soviets and the US-led coalition and had profound involvement in jihadi terrorist activity around Iraq and Jordan.

If we look at this movement from a broader perspective, ISIS ideology appears to be a continuation of that of the jihadi insurgency throughout the Muslim world, which became almost a constant since the last decades of the past century. The reason behind the endurance of jihadi insurgency and ideology, however, stems not only from the continuous longing to restore "the abode of Islam" lost with the fall of the Ottoman Empire or frustration with Western invasions in the Middle East. That frustration and longing are shared by many other Muslim groups, who do not adopt jihadi methods and do not partake in terrorist acts. The cause of jihadi insurgency and ideology longevity then might not necessarily be only in the agenda they promote, but in how they do it and which language they use for that purpose.

Indeed, jihadi methods of warfare and recruitment evolve and become increasingly technologically sophisticated. But the principles and tools of the language they use, from the Maghreb to the Philippines, remain steadily repetitive and similar. Then, the question arises: what is so particular about their language that it, despite the global counter-terrorism efforts, continues to draw recruits and supporters until the present day?

Principles of jihadi language

To begin with, there is its simplicity and clarity. The language they use is very simple and easy to understand. Their message does no dwell upon philosophical or mystical matters in the way many classical Islamic Qur'anic commentaries did.

Amidst the current modern spirit of ideological subjectivism, relativism and re-definition of every phenomenon, their unsophisticated language has a tendency to capture attention swiftly: it gives clear and easy answers to everything. At the time when the West feels increasingly restricted by the nuances of political correctness and linguistic cautiousness, jihadists offer stark linguistic unambiguity.

Second, their language exhibits unchallengeable certainty and confidence. They not only do not question their own principles, but they also express them without any shadow of doubt. One does not encounter a phrase or a statement uttered on their behalf, that they would claim anything other than objective and unadulterated truth. The language they use strikes listeners with unwavering confidence that only their vision is the correct one.

Third, their language is emphatic. Their message is "forced" upon the reader or hearer. Sentences are constructed in such a way, that the act of not accepting them or doubting them constitutes not just unbelief, but also inferiority. If the one considers himself or herself a person of worth and a "true believer", then he or she is naturally expected to agree with their arguments. In a way, their language is provocative, calling one's bluff.

Jihadism is inseparably both religion and politics and its rhetorical techniques find parallels in those of Western political populism. Like populists, jihadists draw stark boundaries between "common people" (true Muslim believers) and "corrupted elites" (Muslim ruling classes). Despite the popular perception produced by terrorist acts in the West, many jihadi ideologues identify as their main enemy not the West, but the political establishment of the Muslim-majority countries. They depict themselves as rebels against the ruling classes, portrayed as disbelievers and betrayers of Islam who uphold a rotten socio-political system. In such a way, the main ethos of their rhetoric is akin to that of the "liberation of the oppressed". In a populist fashion,

they project short, simple, direct messages to provoke an emotional, instead of intellectual, response.

However, if populists in the West use methods of direct democracy to achieve liberation from the establishment elitism, jihadists see the way to liberation through war. Accordingly, they use pro-war rhetoric and their message is constructed to entice very particular emotions pertaining to their cause. People are generally more likely to join the war on the defensive, rather than offensive side, and jihadi language is full of assertions that Islam and Islamic values are under threat. It attacks the "inferior" enemy through undermining its cultural and moral values and contrasting them with an idealized vision of their own. They portray the enemy (anyone who promotes any form of secular ideology) as aggressors and themselves and their supporters (true Muslims dutifully obeying God's law) as victims under attack. To draw others to their cause, their message is permeated with a profound sense of urgency and they accentuate the inescapable conflict in emotionally charged phrases.

"This is Our 'Aqeeda [Creed]": examples of jihadi language

For the sake of illustration of those five principles, let us look at particular linguistic examples jihadists use. Jihadi messages and writings are usually relatively short, especially if compared with classical Islamic scholarly works; they are well-structured, sometimes with bullet-points, and resemble manuals. I shall look at the work written by an influential contemporary Islamic Salafi jihadi thinker Abu Muhammad al-Maqdisi, under whom al-Zarqawi and Turki al-Bin 'ali – the ideological founder and the senior religious scholar of the Islamic State respectively – both studied. Zarqawi developed particularly strong bond with Maqdisi during their five years together in Jordanian prison. Despite the subsequent rift between the teacher and his two disciples, the principles of the language they use are similar.

Born in 1959 in the West Bank

(then part of Jordan), Maqdisi grew up in Kuwait. His family was relatively well-off and, according to his own assessment, not very religious. He was initially influenced by the ideology of Sayyid Qutb and Muslim Brotherhood in their criticism of the Muslim political ruling elites. Later, he also adopted Salafi and Wahhabi religious ideas. He studied in Iraq and Saudi Arabia, and later travelled around Afghanistan and Pakistan; however, he has always been known as a scholar, rather than a fighter, acknowledging his "illiteracy" in the use of weapons. In his very popular book widely circulated online entitled "This is Our 'Aqeeda" (1997), written whilst in a Jordanian prison, together with Zarqawi, for their terrorist activity, Maqdisi explains the fundamental principles to which a true Muslim should adhere. His message is simple and clear. The book is subdivided into short chapters, some of them only paragraph-long, which are easy to follow and comprehend. For some of his arguments he provides more elaborate reasoning, but in an uncompromising and emphatic manner. His manual is a ready-made set of answers, which do not contain complex intellectual endeavors as to how this "truth" was or is to be found: it is here and now, and need only be accepted and memorized. As opposed to the perception that "truth" is an ambiguous and complex subject-matter, he considers truth simple, unequivocal and open to comprehension.

In Maqdisi's view, the primary targets of fighting should be neither Jews nor Westerners, but the "apostate" Muslim rulers of Muslim countries. He calls for unity against the enemy and considers it "obligatory" to rebel against "disbelieving rulers that are emplaced over the necks of the Muslims". The disbelieving Muslims are those who have in any way replaced God's law with man-made laws. Although Maqidsi does not consider it acceptable to wage jihad against anyone without "clear-cut evidence", he still upholds that "jihad is an obligation from the obligations". In the fight against the enemies of Islam, he encourages participants in military operations to "manifest

the radiant image of Islamic Jihad". People who accept his ideology are considered "the people of truth"; those who do not support his ideas are denounced as "enemies of Allah", "deficient" and "those who wage war against the truth".

Referring to intellectually sophisticated language, Maqdisi criticizes it as "adorned speech" containing "deviant thoughts". Intellectual reflection and doubts, especially regarding the validity of jihad, he deems "falsehood" and illegitimate "skepticism". Scholars that provide a more thoughtfully reserved view or employ intellectual arguments are denounced as "evil", who "garnish their falsehood" and "argue with false misconceptions". He fervently insists, that any ambiguities within the Qur'anic text should not be reflected upon or debated – the text must be accepted as it is in its entirety without questioning "how". Militantly arguing against ambiguities, he calls his followers to "believe firm with firm word" and distinguishes them by "having clean heart and tongue".

The appeal of populist language in the West is traditionally linked to economic and social inequalities. Similar reasoning could be found in relation to jihadism. However, in the case of pro-war populist jihadi appeal the reasons are more profound. If Western populism operates within and by the laws of the Western secular socio-political system, jihadi worldview is decidedly antithetical to it. The anxieties and emotional response, which jihadi rhetoric is aimed at, stem from the deep ideological crisis and challenges which modernity is currently facing. This crisis consists of the fact that whilst religion does not have direct and compelling influence on the socio-political order in Western states, in societies and communities throughout the rest of the world it has a much more significant influence on social and political fabric. In fact, eighty-five percent of the world population identify themselves as religious, underlining the dominant role that religion plays in their everyday decision-making.

In those parts of the world, the

western post-colonial nation-state order does not always sit well, for it in principle requires separation of "church and state", "the secular and the sacred", where such dichotomy has previously been non-existent. Before the advance of the Western state system, Islam served as a foundation for socio-political regulations in Muslim societies and therefore the place of Islam in the new state context has become a matter of severe debate across Muslim-majority countries. Such "novelty" in historical terms provokes an acute sense of ideological bewilderment, which jihadists are quick to take advantage of.

That can equally explain the fact that although Protestant North American religious fundamentalist language, for instance, shares similar features of clarity, simplicity, confidence, forcefulness, and populist emotionalism, it does not contain pro-war rhetoric. American fundamentalism developed in the Western socio-political system and by and large operates by its laws. The shift transforming religious and political self-identification in Muslim countries, of which Islamic jihadism is a by-product, had a different timeline and context. If American fundamentalists are part of the Western socio-political system, Islamic jihadists position themselves outside and against it. At present, the appeal of jihadi pro-war populism seems likely to persist. As long as Muslim-majority countries do not find a solution on how Islam should be incorporated into the state fabric, which will alleviate the ideological bewilderment and become widely acceptable and normative, jihadists will continue to have consistent audience amongst those particularly disoriented and dissatisfied with the existing ideological instability on whom their populist language will work. Meanwhile, the linguistic aspect of jihadi appeal should be included in elaboration of a comprehensive counter-terrorism strategy and preventive measures by governments and risk management experts. The efforts so far concentrated on creating a peaceful and positive counter-narrative. However, in view of the ideological instability and absence

of normativity it might not be enough, for the outcome of such efforts is not the elimination of jihadi narrative as such, but existence of two parallel narratives. Countering jihadism linguistically does not only require its denunciation as "toxic" and "evil", as in such case its actual linguistic principles and methods remain unchallenged. A possible strategy for linguistic risk management then might be actual engagement with jihadi messages and public exposition of their linguistic principles so that people can quickly recognize and resist their emotional influence.

Ilma Bogdan is writing her doctoral thesis at the University of Cambridge, working on comparative religious fundamentalist hermeneutics. She holds degrees from King's College London, War Studies Department, and School of Oriental and African Studies. Having background in international relations and diplomatic journalism, her main areas of expertise are the Middle East, contemporary Islam, and the role of faith and religion in the modern world.

At Year End 2017, Will Your Organization Be Protected from Cyber Risks?

We have just passed one of the busiest seasons, not just for the Holidays, but for new business and renewals in the specialty lines insurance business. With the passing of 31 December and 1 January, I wonder if despite the broad knowledge of data breaches and cybercrime if the markets have still not persuaded enough people of the value in buying cyber liability insurance. Recent surveys seem to indicate not. In other cases, it seems that many who are persuaded to buy, may be confident enough to state that they know that they are buying the best coverage for themselves or how to utilize the coverage they buy in the event of an incident.

The past year has seen many major new data breaches making headlines, Experian with over 143 million accounts breached and Uber with 57 million announced more recently, are just a few of the many organizations big and small who have failed to protect private data (and private health information in some cases) from hackers.

In addition, thousands of organizations have been victimized by ransomware holding their systems hostage and while the payments made by many are individually rather small (most historically resolved for about $300 or less), the time that systems are off line has cost businesses millions more in lost income.

Cyber criminals have also been busy. According to FBI data more than $5 billion in losses due to Business E-mail Compromise scams has happened in the past few years. These scams are carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds. The scam has evolved to include the compromising of legitimate business e-mail accounts and requesting Personally Identifiable Information (PII) or Wage and Tax Statement (W-2) forms for employees, and may not always be associated with a request for transfer of funds. The victims of the BEC/EAC scam range from small businesses to large corporations. The victims continue to deal in a wide variety of goods and services, indicating that no specific sector is targeted more than another. Between January

2015 and December 2016, there was a 2,370% increase in identified exposed losses. The scam has been reported in all 50 states and in 131 countries. The FBI has tracked fraudulent transfers to 103 countries.

Nevertheless, numerous surveys, report that close to 40% of US entities are still not buying cyber liability insurance. They seem to believe that insurance coverage is either not broad enough or too expensive in comparison with their expected losses.

Another recent survey conducted by Ovum and FICO, found that of 350 companies polled, less than 50% of US companies purchased cyber liability insurance. The 350 companies ranged in size from fewer than 1,000 employees (30 percent) to over 10,000 (25 percent) with nearly half of them (45 percent) somewhere in between.

Half of U.S. businesses reported having cyber insurance, although only about a third of those (16 percent of the whole sample) were confident that it covers all their risks. Just under a quarter more (23 percent) reported plans to buy insurance in the coming year. The U.S. lags the U.K., where 69 percent report having at least some cyber insurance and 28 percent say it covers all risks. It also trails Canada and Sweden in the percentage who buy and believe it covers all their risks.

Lagging even more — health care. None of the U.S. health care firms questioned in the survey said they had insurance that covers all their risk, while 74 percent reported no cybersecurity insurance at all. (https://www.cyberscoop.com/half-u-s-firms-cyber-insurance-fewer-u-k-canada/)

Given this backdrop, with more than 130 insurance companies offering cyber liability in the USA on a standalone or package basis at different price levels and using quite different policy forms (some on admitted paper and some on surplus lines paper), it is no wonder that many eligible buyers are cautious to part with premium dollars when the benefit of buying coverage is questionable in their eyes. In addition, while large private and governmental organizations have been the focus of the major carriers for many years and many have been able to buy manuscript policy forms, the 5.7 million small and medium enterprises (SMEs) are offered coverage that often seems quite limited in comparison. Also coverages continue to evolve, as

many carriers in their quest for market share are broadening coverages in their policy forms to better help an insured with post-breach costs.

Meanwhile, property/casualty insurers reported $1.35 billion in premium for cyber insurance in 2016. This was a 35% increase from 2015 according to Fitch Ratings. A.M. Best reported that direct loss ratio in cyber decreased from 51.4% in 2015 to 46.9% in 2016. Further, while many buyers are mystified by the premiums, interestingly, recent news indicates that despite the high number of publicized breaches, in most industries, premiums are on the decrease, including in regulated industries such as healthcare and social services, and financial services. A few sectors have seen rate increases, most particularly information companies and for arts, entertainment and recreation. Thus, many buyers are benefitting by the competition for market share among the insurance carriers.

At the same time, many SME buyers question the premiums charged by carriers when they see their risks as minimal or only partially covered by the coverage offered to them. Even some larger organizations are dubious about if the premium is worth paying if the likely loss is such a small percentage of their revenues.

Nevertheless, recent reports from the National Small Business Association (NSBA) for 2015 showed that 42% of small businesses had fallen victim to a cyber-attack. Of small businesses, most who lack significant IT and security resources, only 15% offered cyber training to employees, according to a 2016 Better Business Bureau report. The NSBA also found that the average loss was $32,021. This is often more than many small businesses can afford. Larger accounts have seen many pay millions of dollars to resolve their cyber incidents (Anthem, for example, recently announced one of the largest known settlements for a cyber breach agreeing to pay $115 million to consumers).

For larger accounts (and SMEs that buy the appropriate coverage), having quick access to public relations, breach response services, and forensic services at a pre-event negotiated rate is a major benefit of buying cyber liability coverage even if the limits bought are not adequate in some cases to cover possible losses in

full. However, as A.M. Best has noted, these added-value benefits are costly to insurers and reserved for the largest of accounts at this time. However, if these benefits prove beneficial to loss ratios, they may soon be offered to more accounts at lesser premium levels.

Thus, now that we have passed two of the busiest dates for new business and renewals in the specialty lines business, area many buyers be happy with the coverage they buy and the premiums they pay? If recent surveys are accurate, many organizations will not be satisfied and either view themselves as partially covered or will feel that they are paying premium for little value in return despite a softening cyber liability market and the continued broadening of coverage by insurance carriers. Others, will not buy at all given their concerns and the mysteries of the cyber liability market. Further, many of the SMEs who buy cyber liability will not understand the coverage they buy nor how they can use it in the event of a covered event or buy such small limits as to be insufficient for any real situation.

Would standardization of policy forms help reduce the mystery? Undoubtedly, for some. The Insurance Services Office (ISO) has recently announced its cyber liability form which it offers to carriers for use. If some carriers, most likely smaller and newer to market ones, decide to use the ISO forms and rates, there could be some standardization seen. However, the speed of change in the cyber world and competition between carriers seems likely to make standardization slow to occur in the near term particularly given the expense and efforts made by many of the carriers to offer differential or "unique" levels of coverage to gain advantage in the market. With the speed of change in the cyber world, it may be foolish to think that the changing risks will be able to be standardized any time soon.

Thus, it is increasing important, for many SMEs and even larger organizations to have independent counsel who is familiar with the carriers, the state of the market, how claims work, and how to evaluate the insurance coverages offered to ensure that they are buying efficiently and effectively for their specific risk exposures. Relying on a package policy or on considering only one or two options is not likely to be in an organization's best interest. For those organizations

served by the largest and most sophisticated brokers and buying manuscript coverage, they are already sophisticated buyers. But, for many of the rest, as long as the cyber world keeps evolving, it will be prudent for them to get as much knowledge as possible on their side of the table.

Keith B. Daniels, Jr., J.D. is a graduate of the University of Wisconsin Law School and has worked as coverage counsel handling cyber liability claims, as an underwriter and developer of cyber products for Lloyds of London and US carriers.

He is the founder of CyberCounsel and provides independent advice to carriers in the development of new products and the assessment of market opportunities and to entities interested in an independent evaluation of the adequacy and scope of coverage for cyber and other specialty lines of coverage. He also provides expert witness services.

Sun Tzu and the Art of Fake News

Another word for Fake News is Propaganda and through 2017 we saw so called Islamic State give us a master class in their ability to get their message to the world, whether true or not, they didn't care. Terrorist use of information warfare is as important to their causes as physical attacks and must be understood by those with an interest in security.

You have to remember that the current scourge of Fake News is a cyber enabled activity. As Philip Ingram MBE shows in his article, Sun Tzu and the Art of Fake News, it is nothing new but its methodology of transmission, ability to hit mass audiences and clear ability to influence decision makers is frightening. It is impacting political, business, security, terror and more decision making. It is something all involved in understanding risk and mitigating that risk must think through.

We have seen much over the past year of the new phrase that will almost certainly be seen as one of the major descriptors of 2017 – that is Fake News. It is one legacy that President Trump has already left but why has it come to the fore, is it new and more importantly is it something that individuals or enterprise should be concerned about? Philip Ingram MBE the leading journalist with Grey Hare Media takes a look at fake news, but with a 6th century twist.

There are elements of the press who seem to suggest that fake news is something new, it isn't, and it has its roots back to the 6th century, but before I delve that far back I want to take a quick look to only 74 years ago. The Second World War shows just how important "fake news" was to the war effort; fake news, when targeted for an effect is also known as Propaganda. William Brooke Joyce, nicknamed Lord Haw-Haw, an American-born, Anglo-Irish Fascist who became the Nazi propaganda broadcaster to the United Kingdom during World War II was probably the most famous mouth of fake news, but the Japanese had English speaking female broadcasters who were nicknamed Tokyo Rose.

The use of fake news or

propaganda was not limited to the Germans or Japanese and arguably the greatest military success of the Second World War, D Day, was enabled by fake news through an operation called Operation Fortitude. With this being linked to a military operation this is where I want to bring in 6th century teachings.

Sun Tzu the 6th century Chinese general, military strategist, and philosopher, arguably the greatest military tactician and strategic thinker ever, said in his book the Art of War, “All warfare is based on deception. Hence, when we are able to attack, we must seem unable; when using our forces, we must appear inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near.” His teachings have stood the test of time!

Operation Fortitude was a massive deception operation conducted by the Allied Forces to lead the Germans to believe that they would be landing in Pas-de-Calais and Norway, masking the true invasion through Normandy.

The aim was also to make them believe that the Normandy landings in May 1944 and in the south of France in June 1944 were mere diversions, so that the German army would concentrate its troops in the wrong place. The German authorities clung to their belief that the landing would occur in Pas-de-Calais right until September 1944. Operation Fortitude held onto the principals set out so eloquently by Sun Tzu. The bluff worked but highlights how a country with extensive national intelligence assets looking at a situation unfolding, can be deceived.

The Russian term маскировка (maskirovka) literally masking, was defined in the International Dictionary of Intelligence from 1990 as the Russian military intelligence (GRU) term for deception. Vladimir Putin would have “grown up” in an organization where maskirovka was a normal part of everyday thinking. At every level of my military training we studied maskirovka, so imagine my surprise when Robert Hannigan, the ex-director of the UK spy agency CGHQ, said of the Russian threat in an interview this year, 'We didn't see Russian use of disinformation coming'. It clearly demonstrates a naivety with the UK’s senior intelligence officials, charged with keeping our politicians abreast of the threat to

that which underpins our way of life, democracy.

This failure highlights that those self-same senior intelligence officials have forgotten one of Sun Tzu's most famous quotes. "If you know your enemies and know yourself, you will not be imperiled in a hundred battles; ... if you do not know your enemies nor yourself, you will be imperiled in every single battle."

Should we be worried? Well in my professional opinion, I think we should be extremely worried. This is not just something targeted country on country, it is being exploited by terrorists and so-called ISIS are masters at it, it is being exploited to gain commercial advantage especially when rumors can be generated in the money markets, huge sums can be gained, or lost.

In May last year many respected media outlets reported concerns by the US Securities and Exchange Commission (SEC) over false reporting. The FT outlined that the regulators were concerned that fake news was affecting investment decisions and reported evidence that seemingly independent outlets were being paid to promote stories. They reported the SEC as saying, "keep in mind that fraudsters may generate articles promoting a company's stock to drive up the stock price and to profit at your expense."

Supporters of so called ISIS are very quick to post across their networks details and pictures from any attack, thereby taking de facto responsibility in the eyes of their supporters even before any official statements are released. This has the effect of stimulating potential copycat or other attacks as well as giving "oxygen" to their terror message, to paraphrase Margaret Thatcher. The manipulation of media messaging is extensively used by todays terror organizations.

The one factor that enables fake news to have such a rapid impact today is control, or lack of it. Operation Fortitude was a carefully orchestrated national plan controlled at the highest levels, so all messaging was coherent and worked to a common aim. Today, fake news can be delivered to millions of people at the click of a button via social media and the average person in the street can send a message that the President of the US may read personally, without it going through his normal staffing and advisory chain. The power of

social media is phenomenal.

The Russians continue to use maskirovka as part of their global engagement techniques. We are already seeing proof of their involvement in the US elections and likely in the UK Brexit referendum and more. Sun Tzu highlighted how this works when he said, "Speed is the essence of war. Take advantage of the enemy's unpreparedness; travel by unexpected routes and strike him where he has taken no precautions." Remember, Robert Hannigan said he didn't see it coming and those unexpected routes were Facebook, Twitter, big data manipulation, main stream press and good old fashioned human influence, powered by the internet.

Arguably Kim Jong Un from North Korea knows how to play President Trump using Sun Tzu. As the 6th century tactician said, "If your opponent is temperamental, seek to irritate him. Pretend to be weak, that he may grow arrogant. If he is taking his ease, give him no rest. If his forces are united, separate them. Attack him where he is unprepared, appear where you are not expected." It is this last line that is keeping the world's breath held. Kim Jong Un's understanding of President Trump's temperament is clearly excellent when he applies Sun Tzu's principal, "If your opponent is of choleric temperament, seek to irritate him." Trump gets irritated easily by 'Rocket Man.'

With the ease of spread of fake news and its ability to influence, it is something that enterprise should be concerned about. The instability caused by state on state activity is one thing but there is clear evidence of state on enterprise actions in cyberspace with the theft of IP. Fake news is another cyber enabled activity and the potential for enterprise on enterprise use of fake news is growing.

As an intelligence officer looking at a threat you ask 2 questions. The first, does the capability exist and the answer is yes. The second, is there intent to use it, and again the proof is that the answer is yes. Now is the time for risk managers in companies to ensure the impact of Fake News is something they plan for, remember it is a cyber enabled threat.

In one of Sun Tzu's opening statements he said, "If your enemy is secure at all points, be prepared for him. If he is in superior strength, evade him."

The time has come for preparedness as you cannot evade this threat.

Philip Ingram MBE is a former senior intelligence officer but now journalist who has been writing on intelligence, security and geopolitical issues for some years. He maintains access to organizations who monitor global and terrorist threats. He is a sometime commentator for the BBC on both television and radio and is used by other international channels for professional comment. He runs his own content providing company Grey Hare Media.

Lone Wolf Targeting In 2017: A Suicide Terrorist Can Only Die Once

Persistent intelligence surveillance and diligent law enforcement action make it hard for terrorist plots involving multiple operatives to avoid interdiction. The hostile, well-funded, and well-resourced counter-terrorism environment forces adaptation of the terrorist threat to encompass more lone wolves, who can plan and execute plots essentially without the need for communications that might be intercepted. Just as in the wild, the most dangerous animals are those that attack without fear for their own safety, the most dangerous lone wolves are those on martyrdom missions. They can choose their targeting to cause maximum impact, without needing to consider the personal risk to themselves, or find viable escape routes. Such targeting can be carefully selected in an optimal way: a suicide terrorist can only die once. This is demonstrated by the terrorism experience of 2017, which has been marked by resurgent lone wolves on both sides of the Atlantic.

Introduction

On the morning after the lone wolf terrorist attack on the Arena concert venue in Manchester on the night of 22 May 2017, the UK Prime Minister, Theresa May, declared: 'It is now beyond doubt that the people of Manchester and of this country have fallen victim to a callous terrorist attack, an attack that targeted some of the youngest people in our society with cold calculation'.

The quantitative modeling of terrorism risk has always drawn sceptics who cite human behavior as an erratic limiting factor. Yet the most significant terrorist attacks are not driven by emotion or whim, but have been planned with cold calculation, ruthless and heartless in execution to leverage the maximum harmful impact, and generate 24/7 global media publicity to promote their own terrorist agenda and gain recruits. In this cold calculation, norms of humanity and civilization are set aside; human feelings and sentiments of mercy and pity count for nothing. A suicide attack is itself part of this cold calculation. Such attacks happen as if they were optimized in targeting and timing by a computer program.

For the Islamist, paradise is absolutely assured for the Shaheed or martyr. It is a common perception that terrorists who seek to die in the course of their operations are crazy or irrational. Such a perception is a

form of mind blindness – failing to understand the mindset of others. The 17th century French philosopher Pascal proposed an argument, known as Pascal's wager, to justify sacrifice in the service of God. The probability that God exists is neither zero nor unity. Hence if the reward for sacrifice is everlasting paradise, as Jihadis are convinced, then the expected benefit, (i.e. the product of reward and likelihood), is infinite. ISIS ruthlessly exploits this mathematical logic with the recruitment slogan 'Everyone has to die, why not die a martyr?' Many martyrs leave behind very young children and wives who knew nothing of any terrorist plotting. Counter-terrorism officers understand the practical implication of this ISIS slogan: even those with every human reason for staying alive may be recruited as suicide terrorists.

Optimal targeting for an individual suicide attack

With the $100 billion counter-terrorism surveillance conducted by intelligence services in the Five Eyes alliance of USA, UK, Canada, Australia and New Zealand, terrorist plots involving more than a few operatives have only a slim chance of escaping interdiction. The focus here is on terrorist plots in these English-speaking countries involving a single attacker, having a suicidal intent. Such lone wolves may be self-radicalized, inspired by a terrorist organization, and may have some peripheral contact with other terrorists. Crucially, their modus operandi is to have very restricted communications with other terrorists that might be intercepted and lead to their arrest. In particular, they do not receive regular instructions on carrying out their suicide mission. This contrasts with larger scale centrally-directed terrorist plots, where each cell member may be allocated a specific task, and may not have any choice over their assigned role, or discretion over operational tactics.

Consider the situation where a lone wolf terrorist plot has reached a stage of maturity without drawing the attention of the counter-terrorism or law enforcement services. What then is the optimal target for an individual suicide terrorist? A suicide terrorist can only attack one target. A suicide terrorist can only die once. This is where the cold calculation enters. Terrorists who do not have suicide on their mind can always attack and die another day. Although some IRA bombers were killed through

weapon technical malfunction or counter-terrorism action, IRA bombers planned an escape route for themselves. Those who made good their escape could attack multiple targets in their term of active republican service.

Apart from not requiring an escape route, suicide bombing is operationally more flexible in timing as well as targeting, than planting bombs and leaving them to explode at a fixed time. At 9.30am on September 17, 2016, a bomb exploded near the boardwalk at Seaside Park, New Jersey. The bomb had targeted the end of a charity run raising money for the U.S. Marine corps. But this run was delayed because of a large turnout of around 3000 people - a contingency which a suicide bomber could have exploited to cause maximal carnage. Instead, the planted bomb was in the wrong place at the designated explosion time, and there were no injuries. The bomber had no control over his improvised explosive devices once he left them. Indeed, one backpack bomb was picked up accidentally from a garbage can, and handed in to the police. The terrorist bomber responsible, Ahmad Khan Rahimi, a lone wolf from New Jersey, was convicted of eight counts of transporting and setting explosives, which resulted in a number of injuries, but no fatalities.

The arrest of terrorists like Ahmad Khan Rahimi is a multiple blow for the terrorist organizations that they support. First, their operational failure is a discouragement to others who might contemplate walking the path of Jihad. Secondly, their interrogation can provide valuable intelligence that may assist law enforcement and security forces in stopping further attacks. Suicide terrorists don't talk. This in itself is a boon to terrorist organizations. Any suicide attack that causes some public anxiety and fear, and generates mass media publicity can be reckoned a partial success. But suicide terrorists can expect to achieve greater success through compliance with the following three basic attack criteria

a) ease of execution;

b) alignment with objectives, and

c) high leverage: the ratio of impact to mission cost.

Ease of execution

Occasional gross lapses in security can provide targets of opportunity, but the need for

30

ease of execution generally rules out hard targets, such as senior politicians and other VIPs, who have close personal security. This is not a strategic problem for the lone wolf; there are a multitude of high-profile yet soft targets which have poor security. These soft targets are to be found in open crowded places in major urban areas of high population density.

A rucksack bomb or assault rifle cannot be brought into buildings with bag inspection on entry, or where security credentials and identification are required. Theaters, sports stadiums, concert halls, industrial facilities and large commercial offices and government establishments cannot be readily accessed, unless there is a lapse in security, or if the terrorist is an insider. However, the approach area is typically open to the public and is poorly protected, and therefore a soft target. Approach areas are generally less crowded and more open than interior spaces, which are factors that would tend to erode the intensity scale of the bomb impact. But this is the practical trade-off to facilitate practical ease of execution. By contrast, public transport and the hospitality services have to allow free public access. Accordingly, trains, buses, hotels, shops, bars, cafés and restaurants are open targets for a suicide terrorist, albeit with random security checks.

Alignment with objectives

One of the functions of the leadership of a terrorist organization is to set objectives with which its followers can identify. For all Islamists, the Jihad against the crusaders is a universal attritional long-term objective. Whatever is damaging to the interests of the crusaders is a positive gain for Islamists. The greater the grief suffered by citizens of the Five Eyes Alliance, the greater is the Islamists' celebratory Schadenfreude. The religious injunction to avenge perceived injustices suffered by Muslims is an objective to which all Jihadis are aligned. For ISIS, the command to wage Jihad against infidels is promulgated in its open publication Rumiyah (Rome), which superseded Dabiq, named after the place in Syria designated by Islamists for the final confrontation with the infidels. General advice and

recommendations on tactics for attacks against Crusaders are also offered.

Leverage

Jihadi operations seek to maximize leverage, which is the ratio of impact to cost. The resources available to a lone wolf will vary from one terrorist to another, but achieving a high impact ratio is a key measure of individual success. Collectively, the impact of a terrorist organization is maximized if all lone wolves maximize their own leverage. The historical benchmark for high leverage was set by the 9/11 destruction of the World Trade Center. The economic loss was about $50 billion, and the cost was about $0.5 million, resulting in a high leverage of about 100,000. Impact can be measured in terms of the toll of deaths, serious injuries, property damage, business interruption and economic loss. Apart from these metrics, the societal trauma, PTSD, and fear experienced are important impact factors, as well as the scale and duration of the international media publicity generated.

2017 lone wolf attacks and plots in USA

For a lone wolf terrorist living in the U.S., the weapons most readily available are firearms for shooting victims, and vehicles for ramming them. Obtaining sufficient quantities of explosive for a vehicle bomb remains difficult, given access controls to large amounts of bomb ingredients, like ammonium nitrate fertilizer. However, the challenge of making a small bomb is much more surmountable. Like terrorist groups, lone wolves learn from the successes that others are able to achieve elsewhere, not just in their own country, but around the world. This tends to amplify the frequency of similar styles of terrorist attack. Although the mass shooting of concertgoers in Las Vegas on October 1, 2017, was not a terrorist attack, the shooter, Stephen Paddock, was a lone wolf. The fact that 58 died and more than five hundred were injured would not have passed unnoticed by terrorists who might aspire to emulate the deadliest individual shooter in U.S. history.

The Lower Manhattan Halloween attack

Thousands of Uzbek Muslims are jailed for extremism. Fleeing from an abusive regime, some Uzbeks find their way to the West. One Uzbek, Rakhmat Akilov, claimed asylum in Sweden in October 2014 on the grounds of being tortured. Denied asylum, he joined ISIS and on April 7, 2017, he rammed pedestrians in Stockholm, killing five, and seriously injuring fourteen others.

Six months later, on October 31, 2017, another Uzbek national, 29 year-old Sayfullo Saipov, drove a rented pickup truck down a busy bicycle pathway that runs parallel to the West Side Highway, on the western edge of Lower Manhattan, along the Hudson River. His vehicle rampage killed eight and seriously injured eleven others. Had he not crashed into a school bus at Chambers Street, he might have continued his rampage by striking pedestrians on the Brooklyn Bridge, which has long been a terrorist target. Brandishing imitation firearms when he left his vehicle, he was clearly seeking martyrdom. Nine shots were fired by a police officer, which left him wounded, but still alive. He had chosen Halloween deliberately, because he reckoned the traffic density would have been higher. Although Sayfullo Saipov never reached the world-renowned Brooklyn Bridge, the choice of target in Lower Manhattan was optimal for what Sayfullo Saipov wanted to achieve as an ISIS martyr.

The New York City Port Authority pipe bomb attack of December 11

One block from Times Square is the Port Authority Bus Terminal, which is the largest in U.S. and the busiest in the world by volume of traffic. It was thus an optimal target for a suicide bomber. In an underground passage about 200 feet from the bus terminal, explosive chemical in a foot-long pipe bomb ignited during the morning commuter rush at 7.20 am local time on Monday, December 11, 2017. After the ignition, Port Authority police arrested Akayed Ullah, a 27-year-old Bangladeshi native, who had wires attached to his

body. When the police moved in, the suspect tried to set off the rest of his bomb. He was taken to Bellevue Hospital with burns and lacerations. This was an attempted terrorist suicide bombing, with Akayed Ullah's aim being to take as many people with him. This attack was undertaken in the name of ISIS and against the US administration. On the morning of his attack, he posted on Facebook, 'Trump you failed to protect your nation'.

The suspect could have left the pipe bomb anywhere, and made good his escape by foot. But he planned a martyrdom mission; the pipe bomb was affixed to his body with a combination of Velcro and zip ties. Even though the weapon was crudely and hastily made, the target was carefully chosen.

The San Francisco Christmas day plot

On December 22, 2017, a former US Marine, 26 year-old Everitt Aaron Jameson was charged with terrorism offences, relating to an alleged plot to launch a Christmas attack on a famous tourist landmark: Pier 39 on the San Francisco waterfront, at the edge of Fisherman's Wharf. The features which make this venue especially attractive to visitors, and which travel journalists enthuse about, also make it optimal as a terrorist target: the attractive views of San Francisco Bay, the varied family entertainment for children, two-story carousel, presence of seals etc.

Two days earlier, a police search of his home in the town of Modesto, California, found firearms, ammunition and fireworks. Jameson espoused radical Jihadi beliefs, including authoring social media posts supportive of terrorism, communicating with people sharing his extremist views and offering to provide services to such people, including lending his tow truck in the service of ISIS.

San Francisco is a target-rich international metropolis, compared with a rather nondescript Californian town like Modesto, with a population of several hundred thousand and little name recognition inside the U.S., let alone internationally. Modesto has a high rate of violent crime, but is not a terrorist target. It was

worth Jameson traveling the hundred miles from Modesto to find his optimal target. Not just the location, but the timing had to be right. Like all lone wolves, his family had no inkling of his terrorist intent.

Marked out by a giant Christmas tree at its entrance plaza, Pier 39 is a very popular visitor attraction at Christmas time. From prior reconnaissance, the alleged terrorist had known this would be a heavily crowded area, perfect for his attack on Christmas Day. He could funnel people along the pier and inflict large numbers of casualties. He told an undercover agent that he had no need for an escape plan, because he was ready to die. A martyrdom letter denounced President Trump's recognition of Jerusalem as Israel's capital. This is unlikely to be the last such letter addressing Palestinian grievance over Jerusalem.

2017 lone wolf attacks in the UK

In 2017, there were four lone wolf terrorist attacks in England. In an extraordinary year for UK terrorism, on October 17, the director-general of MI5, Andrew Parker, gave a speech on camera, the first for the head of the British security service. He noted that, 'the challenge we face is undoubtedly a stark one. More threat, coming at us more quickly, and sometimes harder to detect.' In 2017, much of this threat emerged from lone wolves, who are harder to detect than those forming substantial terrorist cell networks. An outline is given of the four lone wolf terrorist attacks, identifying the operational advantages of a suicide attack. According to Andrew Parker, nine Islamist terrorist plots had also been interdicted over the past year. From media information available at the time of arrest, some of these were also lone wolf suicide plots. One such plot, involved a Jihadi on the UK terrorism watch list, who was armed with two large knives. He was arrested in the Whitehall government office area on April 27, close in space and time to the first lone wolf attack of 2017 in Westminster.

The Westminster attack of March 22

On Wednesday afternoon,

March 22nd, Khalid Masood drove a rented Hyundai SUV off the Westminster Bridge Road in Central London, and accelerated at high speed into pedestrians walking across the bridge. Several of them were killed, one was thrown over the bridge, four dozen more were injured, some critically. The compact SUV then crashed into railings outside the Houses of Parliament, whereupon Khalid Masood ran through an open entry gate, and was confronted by an unarmed policeman, PC Keith Palmer, whom he stabbed to death. Heading towards the Prime Minister as she was leaving parliament, the terrorist was on a determined suicide mission, and was duly shot dead by the bodyguard of the UK defense minister. But he would have died knowing that by striking at the heart of the UK government, his targeting had been optimal.

The cost of Khalid Masood renting a Hyundai Tucson, and staying overnight at a budget hotel preparing for the attack, was a modest sum of about £150. The two long knives he could have taken from his kitchen drawer. His proficiency with using a knife as an offensive weapon dates back to when he slashed a man's face in a pub, a crime for which he served two years in jail. A later knife assault sent him back to jail for another six month term.

Taking account of the four fatalities and serious injuries, the direct economic losses of this suicide attack are about 100,000 times higher than the cost. Not only was the targeting optimal, the leverage ratio of impact to cost was about as high as for 9/11 itself.

The Manchester attack of May 22

Manchester, the largest city of northern England, features significantly in the annals of UK terrorism. On June 15, 1996, the Irish Republican Army (IRA) detonated a 1,500 kg lorry bomb in the principal shopping district. This is the biggest bomb detonated in UK since World War II. The insurance payout from the devastated Arndale shopping center was about £400 million pounds. Almost all windows within half a mile were blown out. More than 200 people were injured, including some from flying glass. The fact that there were not many more injuries, and no fatalities, is due to the IRA

phoning in a bomb warning one hour in advance of the detonation. From the rubble of the destruction wrought by the IRA bomb, a new Arndale center arose. However, this successfully redeveloped shopping center was still exposed to the threat of terrorism, and was targeted in April 2009 by Islamist terrorists.

From this same Arndale Centre, Salman Abedi, a 22 year-old local Mancunian of Libyan refugee parentage, bought a rucksack on Friday, May 22nd. Shreds of this rucksack were found in the foyer of the Manchester Arena concert venue on the following Monday night. The rucksack had contained an improvised explosive device, assembled by Abedi in a rented apartment, and packed tightly and evenly with screws, nuts and bolts. With his diligence in bomb preparation and cold calculation, he made sure that this was the worst terrorist attack in UK since the London transport bombings of July 7, 2005. Whereas the 1996 IRA Manchester truck bomb caused massive property loss, but no deaths, the suicide bomb attack two decades later caused little property loss, but 22 deaths, most of whom were young. One girl victim was as young as eight.

Not just the concert venue, but the concert date was optimal for this lone wolf suicide bombing. Salman Abedi knew he had only one attack opportunity. As a suicide bomber, he could only die once. A wide variety of international stars perform at the Arena. The 49-year-old Canadian singer, Céline Dion, was booked on June 25, and August 1st. She has a regular show in Las Vegas, which reflects the demographic of her fan base. By contrast, the 23-year-old American singer, Ariana Grande, has a very young global fan base of dedicated Arianators. She has 150 million social network followers on Facebook, Twitter and Instagram. These followers constitute a vast international sounding board amplifying the publicity for any event involving their young heroine. As the American princess of pop, Ariana Grande, was the best concert target. As a measure of the optimality of this well-planned suicide bombing, ISIS supporters rejoiced whilst watching the comprehensive international

media coverage, which was particularly widespread on U.S. networks.

Salman Abedi's two years of business and management studies at Salford University ultimately trained him only to succeed in this singular ultimate project with a tight deadline. The student loans he took out to pay for his university course, including the period after he had dropped out, will never be paid back to the UK government. So the actual cost of the suicide bombing to ISIS, (including foreign travel and procurement of materials for the bombing operation), was essentially minimal. The attack leverage, defined as the ratio of impact to cost, was therefore massive, as demanded for ISIS operations.

The attack on Finsbury Park on June 19

Early on Monday, June 19, a 47 year-old, Darren Osborne, drove a van into a crowd of Muslim worshippers near the Finsbury Park mosque in north London. One Muslim was killed, and nine were injured. The alleged terrorist had expressed a pathological hatred of Muslims. When he was arrested, he screamed at his captors: 'Kill me'. This anti-Muslim suicidal terrorist had driven 150 miles at night from Cardiff in Wales to north London to strike his optimal target: the notorious Finsbury Park mosque. From 1997 to 2003, under the leadership of the radical imam, Abu Hamza, the Finsbury Park mosque was a center of Islamist extremism, and a haven for Muslim terrorists. Richard Reid, the original shoe-bomber, was one of the terrorists associated closely with this mosque, and responsible for its past terrible reputation.

Darren Osborne had no links with any right-wing extremist group. His violent behavior seems to have been the outcome of personal issues. He was known to be a troubled individual who had anger management problems when he drank too much, which he did before his attack. His suicidal intent was confirmed by his sister, who reported that he had tried to kill himself a few weeks before by jumping into a river.

The London underground attack of September 15

On Friday, September 15, 2017, at around 8.20 am, an improvised explosive device detonated on a District line London underground train at Parsons Green tube station. The District Line train was just pulling into the small station in southwest London in the rush hour when the device partially detonated in the rear carriage, sending a fireball through the carriage. Twenty-nine people were treated in hospital, or an urgent care center, for flash burns and injuries from the stampede to get away from the train. One woman incurred life-changing burn injuries.

The device had been left in a white plastic builder's bucket inside a shopping bag. The device had a power unit, a fairy lights fuse with an electronic timer attached. Five liters of hydrogen peroxide as well as sulphuric acid had been bought online from his cell phone in the past month from Amazon. Indeed, all the items needed for a Triacetone Triperoxide (TATP) bomb could be bought for under £100 in a single order. This is a worrying security development, because of the remoteness and anonymity of online shopping, and has led to calls from British politicians for better controls on online purchases of TATP ingredients.

There were many hundreds of grams of TATP in the device, and several containers of quantities of metal shrapnel including five knives, two screwdrivers, metal screws as well as a broken glass jar, designed to cause severe injuries and death to those nearby. This was the same explosive as used in the Manchester Arena backpack bomb on May 22. From photographs of the smouldering bucket, the initiating charge exploded, but this failed to detonate the main charge due to incorrect construction.

This was not a suicide attack. The alleged terrorist, 18 year-old Iraqi refugee, Ahmed Hassan, left the train the stop immediately before the Parsons Green station. A strategic disadvantage of leaving his bomb was that he had no control over where the train was at the timed moment of detonation. Fortunately for the passengers, the train was stationary at Parsons Green station with its doors open. Had

the detonation occurred earlier, whilst the train was outside Parsons Green station, ready escape from the explosion would have been impossible, and the casualty toll would have been very much higher. Since this was not a suicide attack, the terrorist did not aim to strike an optimal major Central London station. Ahmed Hassan was an unruly teenager, and kept getting into trouble with the police. The choice of the small suburban station, Parsons Green, for IED detonation may have had some connection with his prior arrest near there several weeks before.

Conclusion

A standard terrorism insurance scenario used for Probable Maximum Loss assessment is a large truck bomb detonated in the center of a major metropolis, such as a bomb several times larger than the IRA 1,500 kg ammonium nitrate bomb that devastated the Arndale Centre in Manchester in June 1996. The Manchester terrorist attack of May 22, 2017 demonstrated that a suicide bombing involving a modest quantity of TATP explosive that can be improvised by a lone wolf in an apartment, can kill several dozen people and cause a massive societal impact, and generate global sustained media coverage.

Notwithstanding the 1996 property catastrophe loss, the Prime Minister spoke for the British nation in referring to the May 2017 attack as the worst that Manchester has experienced. Universal public revulsion to this cold and calculating heartless attack suggests that attacks that kill people will continue to be prioritized by terrorists seeking to inflict maximum harm. Indeed, there has not been a successful Jihadi vehicle bomb attack in UK since 9/11, although there was a car bomb plot targeted at the Arndale center in April 2009. Even then, to boost the casualty rate, suicide bombers would have been posted to intercept those fleeing from the car bomb explosion.

As demonstrated by the terrorist attacks and plots against U.S. and U.K. in 2017, the weaponry readily accessible to lone wolves include knives, firearms, small bombs, and vehicles for ramming. Where there is tight

security on the purchase of large quantities of explosive material, it would be very difficult for a lone wolf to perpetrate a vehicle bomb attack. The Norwegian white supremacist, Anders Breivik, did manage to vehicle bomb Oslo government offices in July 2011, at a time when the Norwegian authorities and general population were oblivious to this domestic threat source. Farm neighbors knew that Breivik's use of fertilizer was suspicious, but failed to draw police attention to his unusual behavior.

At his trial, Anders Breivik declared that he embraced death, and looked at his action on July 22, 2011, as a suicide mission. He had not expected to survive. Lone wolf terrorists who launch attacks that do not involve a suicidal intent are less of a public threat than those who do not plan to escape afterwards. Non-suicide individual attacks can resemble regular violent crime. For example, on October 1, 2017, a Somali refugee and ISIS supporter struck a police officer with a car outside a sports stadium in Edmonton, Alberta, and then repeatedly stabbed him before fleeing the scene. Serious attacks on individual police officers are not uncommon crimes. However, as shown by the events of 2017, lone wolf terrorist suicide attacks are far more potent because they can be optimized for maximum impact, without having to trade impact for personal risk.

Indeed, the modus operandi of the lone wolf suicide terrorist can be extended to attacks involving several operatives. On the evening of Saturday, June 3, 2017, a white transit van carrying three Islamist terrorists rammed a score of pedestrians on London Bridge. In keeping with terrorist tradecraft, reconnaissance had been undertaken shortly before to check for any police security on the bridge.

When the van was brought to a halt, the three terrorists ran into the nearby Borough Market, one of the most popular and renowned food and drink markets in London. There they stabbed people, shouting 'this is for Allah'. The attack took place at a crowded place of public enjoyment on the busiest night of the week. Within eight minutes of the police being called, the three

assailants were shot dead. The victims of this terrorist rampage included 8 dead, 48 requiring hospital treatment as well as dozens of walking wounded. As with the Manchester Arena attack, the large loss to society is a large gain to ISIS. Their supporters celebrated all through the night with the customary devilish Schadenfreude, which is a hallmark of ISIS.

Business interruption insurance coverage

The Borough market was closed for eleven days following this terrorist attack, which caused serious harm and distress, but resulted in little actual property damage. Psyched up on martyrdom before they left on their suicide mission, the three Jihadis would have known that they would die in the Borough market. Had they not been suicide terrorists, they could have fled their van after ramming people on London Bridge, and disappeared into the crowd. Borough market would then not have been impacted.

The simple truth that suicide terrorists can only die once motivates them to attack targets which result in maximum impact, for the limited resources they may have. This impact includes economic dislocation, and business interruption, as well as causing as many casualties as achievable. As Prime Minister Theresa May implicitly stated after the Manchester Arena suicide bombing, a high casualty toll is a worse loss to society than property catastrophe damage.

For businesses located in and around crowded public spaces in major metropolitan districts, the prospect of a lone wolf terrorist targeting their neighbourhood constitutes an enduring financial risk for which an insurance solution might be desirable. Given the diversity of possible targets in urban areas, an insurance market for such coverage should be viable. Provided the deductible excludes the most common micro terror attacks, such coverage could be affordably priced for small and medium sized enterprises.

Dr Gordon Woo is a Catastrophist at RMS and is also one of the Co-Founders and Editors of the Journal of Terrorism and Cyber Insurance.

Gordon Woo specializes in the assessment and management of extreme risks, both natural and man-made. He has focused on terrorism risk since 9/11, and is the chief architect of the RMS terrorism risk model. For his innovative work on terrorism insurance risk, he was named by Treasury & Risk magazine as one of the 100 most influential people in finance in 2004. Since 2009, he has been a regular speaker at courses at the NATO Centre of Excellence for the Defence against Terrorism. In September 2013, as a leading international authority on quantitative terrorism risk assessment, he was called to testify to the US congress on terrorism risk modelling.

He has written widely on terrorism, including for the National Defense University in Washington DC, and has authored of the two books: The Mathematics of Natural Catastrophes (Imperial College Press, 1999), and Calculating Catastrophe (Imperial College Press, 10th anniversary of 9/11). Dr. Woo was a top graduate at Cambridge University, completed his PhD at MIT as a Kennedy Scholar, and was a member of the Harvard Society of Fellows. He is currently an adjunct professor at Singapore's Nanyang Technical University, as well as a visiting professor at University College London.

Insuring the Perfect Cyber Storm

The cyber insurance marketplace is poised for explosive growth. With a market value of over $3B in 2017, estimates place the value in 2020 over $7.5B. With this anticipated growth will likely come an uptick in claims. Insurance companies are assessing new ways to help mitigate claims by partnering with leading technology companies and assessing how to improve the application process. In virtually every major data breach in the news, the victim companies looked at "cyber" as exclusively an "information technology" challenge. Recent regulatory requirements from Europe as well as revisions to the U.S. markets and even new conditions set forth in Latin America all point to the probability of increased penalties and sanctions that will correspond to increased claims.

With the pervasiveness of Internet of Things (IoT) and cross functionality of cyber risk with autonomous vehicles, more opportunities will exist for malicious actors – including terrorists, to cause harm to insured parties.

While today's focus appears to be an approach of "write the policy and worry about the risk of claims later", leveraging current approaches in determining what questions on applications and highly relying on technology solutions to reduce risk may lend itself to increases in future claim value and volume.

This information provided in this paper is predicated upon data collected between 2015 through early 2018. This data will provide insights as to current approaches and highlight opportunities to improve upon the manner in which insurers can gain greater market penetration and without increasing their exposure to future claims.

To understand the some of the challenges seen in underwriting cyber risks, we must take a step back in time. From 2012 through 2014, the U.S. Department of Homeland Security hosted a number of working sessions[1] where cybersecurity professionals and insurance stakeholders convened.

The goal of these sessions was to

identify obstacles to expanding and improving the cybersecurity insurance marketplace, which resulted in three ideas for overcoming the identified or perceived obstacles. The first idea was an anonymized cyber incident data repository. The second idea was to develop cyber incident consequence analytics and finally, develop an accepted approach for fusing cyber risk into traditional Enterprise Risk management (ERM).

At first glance, these three ideas have merit and would add value to not only the insurance side of the equation but also improve daily operations of cyber related matters likely driving greater efficiencies in process.

As of March 2018, the current status of each idea remains in continued discussions. While the DHS working sessions have continued well beyond 2014, the ability to execute what was identified as needed is where progress has not advanced as originally hoped for.

If we look at the first idea of an anonymized database for cyber incidents, a couple of issues have been raised. First, who is paying for it? DHS made it clear in 2015 and 2016 they would not be funding the implementation nor the operations and management of such a repository they affectionately call "CIDR" (Cyber Incident Database Repository).

The rationale was not a lack of interest or seeing value, but to remain agnostic and DHS had concerns that some organizations may feel less inclined to share data with a government entity. The second challenge is a fairly longstanding view that sharing of some data may constitute legal hurdles such as antitrust.

DHS communicated they desired a business entity to fund this level of effort because of the good it will yield for all industry. While the funding models remain open for discussion, a goal is to make the data freely available. One option that could resolve these obstacles is an insurance sector Information Sharing and Analysis Organization (ISAO). Because ISAO's are a result of a U.S. Congressional mandate, there are inherent legal barriers providing statutory limits of liability for sharing information with an approved ISAO.

ISAOs are becoming increasingly more pervasive in specific sectors

like healthcare, finance, and even advanced manufacturing. Perhaps now is the time to consider a similar model for collecting and aggregating data for the insurance sector.

To design the analytics for cyber incident consequences requires an agreed upon methodology. The primary stakeholders include Government, Academia, and Industry. Each stakeholder has what they desire to be analyzed and so far - no consensus has been reached.

The last idea is near and dear to my heart as I firmly believe the primary issue we experience today in addressing cyber threats is we treat it exclusively as an information technology "IT" matter and not as an enterprise risk. More and more headlines tout boards of directors are increasingly more concerned about cyber threats and they are looking to buy more cyber solutions to mitigate their exposure.

This approach still aligns with cyber being an "IT" matter versus an organizational matter.

To paraphrase a line from the movie "Moneyball", business owners' goals shouldn't be about buying technology it should be about buying down their risk to a level that is acceptable.

More money is spent on cyber technical solutions today than ever before yet our risk posture is not improving proportionately to the level of spend. So at a certain point you must ask, "Do we fault the players, or the model?"

In 2013, an article by Tony Bradley featured in CSO Magazine Online titled "IT security spending continues to rise but does it matter" hits on this very topic.

In the past 8 months, AIG, MARSH and Willis Towers Watson have all announced partnerships with cybersecurity products and service providers. This is certainly a step in the right direction. Adding capabilities in to the mix with traditional approaches where a battery of 10-20 questions with a binary response of "yes or no" dictated policy premiums, exclusionary provisions, and retention rates is a good thing.

A number of interviews I have conducted while writing for CSO Magazine [2] has supported that while the adoption rates for standalone cyber policies is increasing, it is barely a rounding

error when measure against the larger Property & Casualty lines. This factor and concerns that agents and brokers struggle to convey a meaningful argument to clients as to why "cyber insurance" [3] are attributed to an approach that lends itself to an opportunity for the cyber industry to work with the insurance sector to help provide training.

The goal should not be to make agents and brokers cybersecurity experts but rather to have enough knowledge transfer to ensure the ability to translate the cyber issues into a business risk value proposition.

While discussing this topic with a senior vice president with a midsize insurance agency, it was conveyed that they believe 40% of brokers complete the application on behalf of their client.

While not all companies are the same, if brokers can utilize a tool that is easy to understand and automates the processes and thus reduces the level of effort in reviewing questions on policy applications, there is a win-win opportunity.

If the presumption the market improves to $7.5B [4] in just two short years is accurate, where will these premiums originate? The top five firms? Perhaps mid and small market players make up the balance in the aggregate? Regardless of how you examine these numbers, the ability to adequately convey to an insured party they need cyber coverage is still an area of concern, especially to small business owners. Many small business owners feel they are "too small" to be targeted and as a result, have no need for coverage – even in the face of overwhelming data to support the contrary.

Many insurance professionals are well versed in fire, flood or theft coverages but cyber is a challenge because of the following:
1) It is not a subject most agents and brokers feel comfortable with.
2) Cyber is very dynamic.
3) Network interdependency causes issues in defining better first and third party liabilities.
4) Business owner optimism bias "it won't happen to me".

I would argue that points 1 and 4 are directly linked to one another.

The challenge for the industry is not just the cyber element by the

"interdependency" of cyber against multiple lines of coverage.

- Auto (Autonomous vehicles)
- Property (Facilities management and IoT devices)
- Airlines (passenger details and GDPR requirements)
- Medical Devices
- D&O (Recent Uber case could be new benchmark where public information supports intentional and willful wrongdoing and does that negate coverages for cyber since cyber was the original harm trigger?)
- Terrorism

I want to spend more time on terrorism for a variety of reasons but the primary reason is the rationale for covering acts of terrorism. Just a few years ago, policies had exclusionary languages for terrorism and now they are almost barricaded in the four corners of any major policy. Why is that?

To address issues associated with terrorism, the United States came up with a mechanism to create statutory limits of liability known as the "Safety Act". Essentially you demonstrate compliance and you receive a certificate from the United States Government and the intent was to dramatically limit the financial risks associated with claims brought against a business for negligence being the catalyst for the terroristic act.

As with many ideas like this, how they are thought up versus executed may not necessarily align. For an act to be denoted as "an act of terror", only the Secretary of Homeland Security and Director of the Federal Bureau of Investigation can make that ruling.

Even if you have cybersecurity products with the Safety Act warranty, how likely is the DHS Secretary or FBI Director to state that a computer attack on your insured party's was an act of terrorism? More and more attacks are being singled out as nation state attacks but not terrorism for the most part.

To conclude this portion of this article, I would be remise if I did not cover the topic of what are the insurers doing with your applicant data. In 2017, the National Association of Insurance Brokers (NAIC) ratified an administrative law

to enhance the protections of consumer data while in the hands of the insurers. This law generally aligns with a law from the State of New York's Department of Financial Services (NYDFS)[5] with some caveats.

In addition to the NAIC Model Law, on May 25th, 2018, the General Data Protection Regulation (GDPR) goes into effect and has profound implications to insurers that maintain European Union (EU) residential data. Many firms in the U.S. take the misguided position that this EU law won't have enough teeth to reach across the Atlantic. It is important to note that the "mechanism" allowing these same firms to acquire these data sets is through a program known as Privacy Shield, formerly known as the Good Harbor Act.

The Federal Trade Commission has already announced in February 2018 three active investigations into U.S. businesses for violation of Privacy Shield [6]. Once May 25th rolls by, it appears that the FTC will be the enforcement arm of this new GDPR mandate here in the United States.

As the regulatory landscape becomes more stringent, the value and volume of claims will likely go up. So even if we get to $7.5B by 2020, how much impact to insurer's corporate bottom lines will take place and how can the insurance sector hedge their bet to offset some of these costs?

Conclusion

To get from $3.3B to $7.5B in two years will require the following to take place. First, the majority of agents and brokers will need training to understand how to translate cyber threats into business risk, thus costs of ownership. This cannot be done simply by looking at "IT" alone.

Cyber risk must be conveyed in a manner that is comfortable to the agent/broker while simultaneously positioning it as a business peril no different than flood, fire, or theft. Conversely, these same stakeholders will need proper training on regulatory reform in protecting consumer data and how to limit their employers to civil actions for failing to meet their fiduciary obligations

under the standard of care.

Second, to date, there is no one unified repository for cyber claims like the one used for automobile insurance leveraging automobile vehicle identification numbers and drivers' license data. The industry must find a means to evaluate the cyber risk profile of applicants in a way that can change as the cyber threat landscape changes.

There is a value in using technical solutions that leverage algorithms, assess corporate domain settings, or potential malware propagation, but the time has come to understand these approaches are sometimes generating false positives and fail to identify the "causation" of a claim. Implementing an ISAO style model will allow the insurance sector to obtain data "pre-event" and potentially enable correlation between how an application is completed, how an insured party addresses cyber hygiene and how these two data sets can be used to predict a cyber incident more rapidly and reduce a potential claim.

Many insurance stakeholders highlight the "Amazon Cloud" being hacked as the perfect cyber storm scenario. I respectfully submit a more likely scenario are high value claims resulting from regulatory sanctions.

The fact an insured party gets hacked is no longer a de-facto position of negligence. Courts have moved to a position of all companies will get hacked but how well did they respond and recover? This is where privacy laws kick in and actions not by the "individual" but by State Attorney Generals, Federal Trade Commission, NYDFS, EU Commission, and so on. Regulatory authorities with the authority to levy billions in penalties and all the time and resources to pursue.

Finally, just as the firm JLT recently designed specialized cyber policies for airlines, just as many other firms have specialized lines of coverage, the ability to properly denote policy crossovers from cyber to auto, D&O, etc. is a critical step in to reduce exposure.

To conclude, these are challenging and exciting times for the insurance industry and there is tremendous growth in

cyber. The trick will be to apply lessons learned, accept that what got us to $3.3B will not get us to $7.5B without consequences to bottom lines and the recommendations described here are viable in today's marketplace.

Carter Schoenberg is the President and Chief Executive Officer of HEMISPHERE Cyber Risk Management. Mr. Schoenberg is a Certified Information System Security Professional with over 24 years of combined experience in criminal investigations, cyber threat intelligence, cyber security, risk management, and cyber law.

Mr. Schoenberg started his career in law enforcement as a homicide detective but also has experience in both public and private sectors. He has had experience working with the U.S. Departments of Homeland Security and Defense, the Information Sharing and Analysis Center (ISAC) communities, and the Georgia Bar Association for Continuing Learning Educational (CLE) credits on the topic of cybersecurity risk and liability. He has spoken at a variety of global conferences on the issue of cyber security.

The Illusion and Reality of Silos: The Role of Insurance Within A Broader Security Paradigm

"Risk comes from not knowing what you are doing. Price is what you pay. Value is what you get. Someone's sitting in the shade today because someone planted a tree a long time ago."
Warren Buffett

Risk comes from not knowing what you are doing. Price is what you pay. Value is what you get. Someone's sitting in the shade today because someone planted a tree a long time ago. (Warren Buffett)

These words are very apt in describing today's security environment. Essentially, the more that we put in today, and the more that we work together in generating holistic solutions, the better the results in the long term. This article focuses on the role of the insurance industry in the delivery of security solutions by protecting the financial and economic aspects of the risk.

Insurance is a security measure. Yet all too often the contribution of insurance within a holistic security strategy is not recognised, and it is treated instead as a silo. It is now coming to be generally recognised within the security profession that cyber security should not be treated as a silo within an organisation; rather, it is everyone's business, and 'converged' security solutions are necessary. Insurance needs to be considered in exactly the same way.

One means of conceptualising the problem of existing silos and generating a change is firstly to look at how we tend to conceive the security profession. This of course includes corporate and commercial security practitioners, both generalist and specialist, police and law enforcement professionals, intelligence operatives and military personnel. However, we also need to see that within the broader ambit of those who provide solutions to security breaches we have insurance providers, lawyers and others whose work touches or affects security outcomes and are working within government and large corporates. The integration of

these people/ professionals who may not have been traditionally been considered as security personnel (in the broadest use of the word) is likely to involve a multifaceted approach. Integration and collaboration involves an openness to embrace things new as well as a receptiveness of those who are within the existing security professional to accept the openness and willingness to collaborate and integrate. The professionals whose work either directly or indirectly touches or affects security related issues can start by involving themselves in broader security agendas as well as joining or becoming involved in broad sector security groupings or organisations such as the Security Institute. However, if these individuals are willing to join and become recognised as members of or players within the broader security paradigm, a request is made that the existing sector or security industry be receptive to this. This modernised grouping involving professionals who play a role in overall security solutions will enhance the overall security of a company, entity, government and promote safety and resilience of people, communities and businesses.

Given that security threats and the development of solutions to address these involve a wide array of individuals offering different services, it is best to look to a holistic solution rather than a set of silos dealing with individual facets of the problem. When there is a lack of collaboration and an entrenchment of the silos there is a duplication of resources and an escalation of costs and, even worse, the danger that certain threats will fall into the cracks between them.

The insurance industry is one of those resting on the outer edge of the security industry, not always certain of its place within the security sector. Many insurance companies are opening up to and seeking to engage with the security industry. Greater knowledge, learning and mutual benefits will emerge from breaking down the existing silos and generating a more communicative experience.

Taking the example of cyber insurance, my own specialism, as we innovate, adapt and develop product and service offerings, we are seeking to be part of a holistic security experience. Although insurance is critical to the economic security of a company, entity or individual after a cyber attack, we do of course recognise

that insurance alone is not enough. In order to address cyber risks, we seek to develop a joined up approach where we can look at the problem of cyber threats and its transformation in a multifaceted issue and respond accordingly.

Insurers have the best possible understanding and insight into providing economic protection against business risks. In terms of physical risks there is often a convergent of physical risks and cyber risks. In some cases, the physical risk within the cyber setting for example, may be access to a building, hardware, access to computer systems or servers or the ability to use USB devices for example. Even in a risk which we do not often think of as having a physical aspect, there is a very clear role for physical security. In the same example, there are possible physical implications arising from cyber events or cyber intrusions which necessitate the involvement of physical security professionals. Using this cyber example, often the understanding of the physical risks is also important to understand the technical risks and the possible ways in which security can be breached and the manifestations of such potential breaches. In addition, to understanding the surrounding security of a building, infrastructure or assets and the physical aspects of the risk, in the example of cyber, the insurance industry would also very much rely upon technical cyber professionals who have the specialist knowledge of the IT and cyber infrastructure, vulnerabilities and programming capabilities, and can generate patches or other technical solutions. The ability of insurance, physical security and technical cyber experts in this example to work together to generate a holistic solution, will be preferable to a pure economic solution. The economic solution, coupled or entrenched within a broader security strategy will however aid the recovery and enable a company or entity after a cyber event or other security event to have the cash flow required to continue their operations. A solution that just concerns itself with the physical risks to a building or assets (including computer systems and servers), a pure insurance solution or technical cyber security of its own would not be optimal; such solutions just look at one limb of the problem. Security problems or security breaches manifesting in losses rarely affect only one part of a business or institute rather they are more likely to have

impact across several areas of a business and may even affect the overall functionality and operability of a business (even if only temporarily). However, a collaborative and joined up security program of reducing physical and virtual risks as well as an economic backing to promote with resilience and recovery is preferable and this takes into account minimisation, prevention, minimisation and recovery from security breaches.

Intelligence gathering as well as physical surveillance can monitor individuals, groups, potential state actors or others involved in generating the greatest physical, cyber or other security threats and the broad threat groupings. Law enforcement has a role in dealing with the criminality, primarily after it happens, and prosecuting where possible those engaged in cyber crime.

In order to enable the comprehensive protection of people, businesses and communities, insurance is necessarily part of the solution. As well as dealing with the financial and economic impacts of a risk, it encompasses support services in the recovery process. In order for insurance to work effectively, insurers need to work closely with our security peers in order to be able to understand the specifics of the physical, cyber and other security threats that are facing businesses, individuals and communities, for example the state of its evolution and key threat actor groups, how they are likely to perpetrate an attack or disruption and the manifestation of this. The manifestation of the attack or disruption like the security strategy needs to take into account the overall impact as well as direct or indirect impacts to a particular department or arm of a business. This information required for the holistic security strategy, likely attack vector, and resultant outcomes will arise from intelligence gathering as well as those who understand technical intricacies and those who can monitor physical security threats. With all the key players working together, including the police, we have an opportunity to minimise the impact of future events and create solutions that look at the problem from inception to prevention and, if there is a physical intrusion or an attack on a computer or computer systems in a cyber example, address the remediation and recovery. The joined up approach will also help facilitate the identification of patterns used by adversaries to carry out attacks and put in place

solutions to combat these and isolate any potential losses. Collaboration is the strongest force we have available.

In terms of this collaboration, the first thing is to enhance the awareness of the different approaches and the benefits from a more joined up approach. This will be cost and time efficiencies as well as an enhanced likelihood to prevent many more security breaches whether physical or virtual. One way of achieving this is for those involved in the various security solutions can seek to work together to create blended solutions. For the purpose of consistency, again using the cyber example, this will involve security solutions which take into account physical risks and ways of minimising these risks, cyber professionals being more prescriptive about what clients and stakeholders must do and how regularly in terms of ensuing their systems are as safe as possible as well as adequate and adapted insurance solutions. The bringing together and selling of such products and services will benefit all of those involved but it will also be more advantageous to a company or individual as opposed to having to source a multitude of different security solutions individually from a variety of different providers which is tine consuming, can be confusing in terms of what is available and what is needed for the individual business risks and also more expensive for all involved including those buying as well as the business costs associated with such products. In terms of both the provision of security as well as the level of insurance cover offered, it is likely a higher degree of security will be offered at a more reasonable rate and in terms of the insurance solutions, it is likely cover with higher limits or more extensive insurance products will be offered than companies who do not engage in such security priorities or who do not understand their risks, vulnerabilities and the variety of different mechanisms they have employed to resolve or to combat such threats.

More broadly as a means of working together, there should be means whereby each of the different sectors of the security community can educate each other and can learn from each other. This can be done formally through a security organisation such as for example the Security Institute or more informally within a company or within a sector. A future option concerning the ways in which the Security Institute can

facilitate collaboration will be shared in due course. However, opening the dialogue between the different sectors, is likely to also create new business opportunities for all involved. Essentially, whenever there is a breach of security whether it manifests itself in a physical, cyber or other medium, it is in everyone's best interest that the breach or disruption is contained, minimised and a strategy for resilience and returning to a state of 'business as normal' as soon as practicable is not just a business but also a broader societal objective.

The breaking down of traditional barriers to promote a joined up approach also sends a very powerful signal to our adversaries. Together we are stronger, and by sharing knowledge, we make it harder for the adversary to exploit the gaps where information does not filter through from one silo to the next. Instead, it provides a stronger position from which to analyse past events, learn and adapt so that we can be resilient in the future. Ultimately if there is a loss, it is best that everyone is on board from the security sector, as ultimately the only winners from these events are the cyber adversaries who have been able to exploit our own entrenched silo system to their advantage. This is therefore a plea to take guidance from the words of Warren Buffet and start to plant the necessary seeds now.

In summary, security is an encompassing profession which is, in essence, about the safety of people, business and communities. Insurance is a part of that solution which is also concerned about all of the different elements of the solution. It provides the added economic and financial buffer. As the year is yet young, let this year stand for a turning point whereby there is greater, collaboration, adaptation and modernisation of the way various security risks are perceived and remedied. Let us become a united forced for the future and a seed of resentment for our adversaries carrying out security breaches. Using the example deployed in this article of a cyber event, cyber attackers will come to realise that they are faced with a harder task of continuing to carry out cyber attacks or other security breaches when confronted with a united security paradigm which covers physical, technical and economic and financial (through insurance) aspects of risk management, mitigation and recovery.

Dr. Rachel Anne Carter MSyI is Director of Research and Policy at the Security Institute, and Managing Director of Carter Insurance Innovations Limited. Rachel is the Manager and Co-Founder the Journal of Terrorism and Cyber Insurance. She is also a Managing Director for Carter Insurance Innovations Limited, a consulting firm specialising in terrorism and cyber insurance.

Her prior experience working in terrorism insurance and natural disaster insurance includes working for the CEO of Pool Re within a research capacity. She was also involved in Cyber Innovation (Underwriting) at AmTrust. Rachel began her terrorism insurance career as an insurance consultant for the OECD. During her time at the OECD she was instrumental in designing and implementing the E-Platform on terrorism risk insurance. She has also worked at Tokio Marine Kiln and Lloyd's. Rachel holds a PhD in Insurance Law.

LEGAL

The Journal, its Management Team, Advisory Board and Sponsors do not purport to provide any advice which is legally binding in the process of producing or disseminating the Journal or any in- formation contained within the Journal and should not be relied upon as a sole basis upon which insurance policies are underwritten. It is the expectation that each (re)insurer will do their own due diligence and use the information merely as an aid to understanding the risks and landscape upon which terrorism and cyber insurance is currently offered. Any information provided by the Journal should be used solely for educational purposes. The Journal cannot guarantee the accuracy of all detail within individual articles, rather the contributors individually guarantee the authenticity and originality of the work contributed. Further any of the contributors in providing an article, warrant that the Journal is their own work and does not breach any laws including copyright and/ or intellectual property laws.

Legally and from an operational perspective, the Journal is a neutral central party used to coordinate ideas, research and promote innovation. The Journal retains the legal rights to republish the research, infographics and any images provided to it from contributors, however each contributor may seek the permission of the Journal to subsequently publish their work in other mediums. Similarly, if the article has been published previously in a similar format the author warrants that they have permission to have the article republished in the Journal.