THE JOURNAL OF TERRORISM & CYBER INSURANCE

WWW.TERRORISMCYBERINSURANCE.COM

TEAM@TERRORISMCYBERINSURANCE.COM

THE JOURNAL OF TERRORISM & CYBER INSURANCE

WELCOME

The team at the Journal of Terrorism & Cyber Insurance (Rachel Anne Carter, Raveem Ismail, Gordon Woo, Padraig Belton and Tom Johansmeyer) are proud to bring you the second issue of the Journal of Terrorism and Cyber Insurance. We focus on a number of issues including:

- Crowded places terrorism initiatives.
- Cyber aggregation and impact for insurers.
- Cyber disruption.
- Chemical risks associated with terrorism.
- Defining terrorism and other legal challenges.
- Media influences on terrorism.

We are also featuring a new section of the Journal which encompasses comments on the terrorism and cyber insurance market 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.

Since the launch of the Journal in October 2016, it has been evident that there is an increasing need for a publication like this, aiming to inform the market in niche but increasingly relevant areas such as terrorism insurance, cyber insurance, the insurability of drone, self-driving cars, etc. The internet shows a constant stream of potential terrorist events which have been foiled or arrests which have been made all over the world. In Europe, there is uncertainty in Britain, with the fear and division accompanying Article 50 which will trigger Brexit. In France and Germany, events have evidenced a growing radicalisation of some populations and growing extremism, fear, manipulation and 'fake news' in the lead up to the elections. There is increasing frequency of terrorist activity within Asia (with more events being reported from Indonesia, Pakistan and India, as well as direct threats to for terrorist attacks to occur in mainland China). Turkey is under pressure, political uncertainty and fear, as it is continuously subjected to various attacks, bombings and other terrorist related incidents. The situation in Mosul and Syria continues to be strained as the fighting ensues. However, the foothold which ISIL previously had within these areas is likely to be more dispersed. It is therefore likely there will be a greater geographically spread as jihadist fighters are returning to a variety of different countries rather than a concentration in one locality. In the US, the Trump presidency has captured much attention of which the Journal has taken note and included a special section on the potential impacts of the Trump presidency on terrorism and cyber insurance.

Since our last edition in October 2016, there have a number of high profile terrorist attacks including the Christmas attack in Berlin, a New Years Eve attack on a Turkish nightclub, a letter bomb exploding in the International Monetary Fund office in Paris, explosive devices were sent to other European financial institutions. Numerous potential terrorist attacks were foiled before they could be carried out in Germany and elsewhere within Europe. The attack

mechanism illustrates the continued 'lone wolf' trend involving guns and knives, whereby a number of civilians has been injured. There is an increase in the number of 'lone wolf' attacks using vehicles; cars or trucks, as the weapon of choice. The target attacks are to drive into crowds and generate bodily injury, mortalities, fear and panic amongst the people in the affected areas. Recognition needs to be made regarding the media hype surrounding some of these events coupled with fake news sensationalizing some events and calling them terrorist events before adequate consideration and categorization has taken place. The challenge in defining terrorism and also drawing the line between criminality and terrorist acts is a topic that has been explored further by an expert legal practitioner who is also a thought leader in the insurance and reinsurance space.

Although there have not been any chemical, biological, nuclear or radiological (CBRN) events during this period, as players interested in insuring against terrorist events, it is important to remain vigilant and watch and minimize opportunities for future events. To this extent the Journal has engaged in its first educational seminars focusing on chemical and biological terrorism, designed to deliver highly technical information that is targeted and relevant to insurers. Our first event will be held at the City of London club on 31 March 2017. For further information or to register please see: http://tinyurl.com/ChemBioLondon

A comment from one of our CBRN experts, Steve Johnson on the terrorism insurance market suggests 'we face challenges on a number of fronts in terrorism insurance. On one hand there are the continual challenges of state intervention and market penetration. As we see some evolution in the types of attacks and greater uncertainty in their location, perhaps due to displacement effects, we need to get a wider base taking appropriate insurance. The second set of challenges has always been with us, but has become more pronounced; how do we meaningfully model Business Interruption and even Property Damage when the attacks do not leave classic radial impacts.'

Moving to cyber insurance, recently there has been a tendency to question the viability of the existing cyber insurance market and how it can grow and adapt to ensure that it remains relevant and fit for purpose going forward. Recognition has been made that the current market is largely unsustainable and that greater limits are needed for cyber insurance policies. Dialogue has been entered into by key industry leaders about finding alternative solutions and increasing cyber limits through use of the insurance linked securities (ILS). Some government pools (such as Pool Re) are questioning whether it is their duty and the acceptability of expanding their coverage in terrorism insurance to include events where the cause of the physical damage was a cyber mechanism.

In particular, interest in loss aggregation has gained momentum. The transfer of cyber risk to the capital markets – where appetite and capacity certainly exist – would benefit profoundly from the availability of an independent, third-party solution for tracking industry losses, which could then be used to facilitate index-based instruments to ultimately free up primary market capacity. Cyber large risk loss and catastrophe event histories for the global insurance industry may be thin at present, but the potential for future losses remains significant, and the development of a mechanism for tracking and reporting industry losses could address a near-term need, even if such a platform may come relatively early in the cyber insurance sector's life cycle.

All of this discussion is occurring against a backdrop of cyber breaches, exposure of vulnerability and new reporting requirements prompted by changes to regulation (including

those implemented in New York in February 2017). Regulators within Europe are likely to increase the level of regulation in the lead up to the Global Data Protection Regulation becoming legally enforceable as of May 2018.

In late 2016, the US began imposing sanctions on Russia following reported cyber attacks during the November elections. Although a particularly pertinent issue for the states, cybersecurity is not only a matter for states.

At the start of December, German police took down the Avalanche Botnet, one of the largest cybercrime networks in existence. The botnet controlled a network of compromised computers, which it rented out to clients. It also was behind Trojan.Ransomlock.P and Trojan.Bebloh, the last a piece of banking ransomware which targeted German speakers in Germany, Austria, and Switzerland.

Then in the middle of December, three members of Bayrob, an international cybercriminal gang based in Romania, were extradited to the US under the Racketeer Influenced and Corrupt Organisations Act (RICO). This is a first in cybercrime, after a case which had lasted a decade.

The network, according to the FBI and cybersecurity analysts, is responsible for stealing $35 million through auto auction scams, credit card fraud, and computer intrusion. Here and elsewhere, much of the investigative work was done not only by governments and police forces, but by private security organisations like Symantec.

A larger-scale story came to light in August, when an attack group called the Shadow Brokers released a sample trove of data it stole from an NSA-linked cyber unit called the Equation Group, saying it would auction the best files to the highest bidder. It provided a Bitcoin address, and instructed interested parties to send Bitcoin to it. Losing bidders, it said would not be refunded, but would be granted 'consolation prizes'.

It all provides a glimpse into the murky coming world of cybercrime. And it is at any rate an exciting moment for cyber insurance.

2016 saw a 50 per cent increase in policies written against cyber attacks, according to specialist cyber insurer CFC Underwriting. And the total written premium in cyber insurance, currently $2.5 billion, will reach $20 billion by 2025, the Allianz Group believes. Lloyd's of London, for one, sees cyber insurance as increasingly the theme for 2017. The London insurance market introduced 15 different types of cyber attacks coverages in 2016 in anticipation of increased demand next year, says its CEO Inga Beal.

Observers have said cyber insurance has reached a fork in the road, with AIG and AON opting for single-peril policies, covering all losses, including bodily harm and financial loss, that can follow from a cyber attack. Only a few large insurers have the ability to cover this type of risk. Other insurers are focusing on the outcome rather than the cause of the attack; however, the attack is carried out. Unclearly written policies are common, with 'cyber' added on in various places, and insurers not clear what their cyber cover is. Underinsurance is prevalent, both because of these questions of clarity in policies, and more so because only 5 per cent of UK businesses have bought cyber insurance.

In addition to the evolving, changing and increasing cyber threats, new challenges to the man-made catastrophe space are being presented through automated vehicles, including the

challenge to insurance caused by this and the issues of increasing capabilities for drones. Insurers are starting to make demands of the legislators to develop clear legislative guidance to better enable a development of the market and clarity regarding liability. These changes are occurring amidst a move towards automation and the challenges associate with developing new technologies which include that with the development of artificial intelligence, in a matter of years some traditional insurance roles may be replaced by robots.

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

Dr Rachel Anne Carter
Manager and Co-founder, JTCI
Managing Director,
Carter Insurance Innovations
Terrorism & Cyber Insurance
Expert, Security Institute (UK)

Tom Johansmeyer
AVP, PCS
Advisory Board, JTCI

EDITORS & ADVISORY BOARD

The JTCI's founding members, comprise:

- Dr Rachel Anne Carter. Managing Director, Carter Insurance Innovations Ltd.
- Dr Raveem Ismail. Director, (Re)insurance & Analytics, Fractal Industries.
- Dr Gordon Woo. Catastrophist, RMS.
- Padraig Belton. Journalist, BBC, S&P, The Spectator.
- Tom Johansmeyer. AVP, PCS.

JTCI ONLINE

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

team@TerrorismCyberInsurance.com

www.TerrorismCyberInsurance.com

www.terrorismcyberinsurance.com/feeds/posts/default

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

www.Facebook.com/TerrorismCyberInsurance

www.Twitter.com/TerrorCyberIns

2016 LAUNCH AT ARPC TERRORISM CONFERENCE

Our thanks to Dr Christopher Wallace, CEO of the Australian Reinsurance Pool Corporation (ARPC) and Joan Fitzpatrick, Chair of ARPC and the OECD, for graciously hosting the Journal of Terrorism and Cyber Insurance's launch at the October 2016 ARPC-OECD Global Terrorism Conference at Parliament House, Canberra, Australia.

SPONSORS

We are very thankful for the continued support of our key corporate sponsor, Property Claims Services (PCS, a division of Verisk Analytics).

PCS' Tom Johansmeyer stated: "The terror threat is shifting. Adaptation and collaboration is necessary to ensure (re)insurance products are fit for purpose and can be employed to deploy capital efficiently when times are tough... The need for greater focus on improved risk and capital management relative to terror and cyber has only gained momentum over the past year, and the trajectory seems likely to continue. The *Journal of Terrorism & Cyber Insurance* provides a crucial forum for the exchange of thought leadership and commercial insights that can help re/insurers allocate capital more effectively and – more importantly – communities and businesses recover from an event. The role of the insurance industry is to protect the insured and society. The JTCI should provide a forum to help advance that mission."

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 information 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 co-ordinate 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.

Contents

Welcome 2
Editors & Advisory Board 5
JTCI Online....5
2016 Launch at ARPC Terrorism Conference 6
Sponsors 7
Legal 7
In Brief: Commentary From The Industry 11
Short Articles 16
Paris One Year On... Resilience In The Face of Adversity and the Need for Greater Partnership to Promote Continued Resilience....16
Trump & Potential Ramifications for Terrorism & Cyber Insurance 17
The Challenge of Cyber Loss Aggregation 20
Can Insurance Further Define Terrorism Risk Management & Loss Mitigation Credit (LMC)? 23
Long Articles 25
On-Site Risk Surveys with an Aligned Approach for Physical and Cyber Security to Reduce the Potential Exposure from Cyber- Attacks on Industrial Control Systems 25
Defining Terrorism and Terrorist Risk For Insurance Purposes 34
Protecting Against Chemical and Biological Risks to Office Buildings....37
Media Influence on Terrorist Attacks 44
Financial Disrupters: Is The Rise of Financial Disruptors Knocking Traditional Banks Off The Track?....49

Professional Development Seminar
Chemical/ Biological Terrorism: Concepts for Insurance & Risk Professionals

The Journal of Terrorism and Cyber Insurance, in conjunction with Strongpoint Security, a specialty consultancy, are hosting this seminar on Chemical and Biological terrorism and incidents. This seminar will focus both on defining key concepts in ways relevant to the insurance and risk sectors and examining relevant case studies for lessons applicable to a City audience. A panel discussion and extensive Q&A will ensure that attendees get full value from attending.

Presenters include Dr Rachel Carter and Dr. Gordon Woo, both with extensive insurance sector experience and Dan Kaszeta, formerly of the US Army, the White House Military Office and the United States Secret Service, who has over 25 years experience in protecting against chemical and biological incidents both in the military and civil sectors.

Speakers



Date: 31st March 2017 – 9:00am to 2:30 pm

Location: City of London Club

Tickets and Registration Info:
http://tinyurl.com/ChemBioLondon

www.terrorismcyberinsurance.com PCS strongpointsecurity.co.uk

Original Risk

Take a Bite

Tempted by Sustained Profitable Growth?

For more information, please contact:

Tom Johansmeyer
AVP – PCS® Strategy and Development
+1 201 469 3140
tjohansmeyer@iso.com

#originalrisk

verisk.com/originalrisk

PCS

©2017 ISO and the Verisk Analytics logo are registered trademarks and Verisk is a trademark of Insurance Services Office, Inc. PCS is a registered trademark of ISO Services, Inc.

IN BRIEF: COMMENTARY FROM THE INDUSTRY

Pádraig Belton
Journalist, BBC, S&P,
The Spectator

Comment on the Westminster event of 22 March 2017: As this issue goes to press, the United Kingdom begins its discussions of how to respond, in counter-terrorism policy, to the first terrorist attack in London since the 7/7 bombings of 2005, along with the first attacks in the United Kingdom subsequently claimed by ISIS.

Similarly, Brexit poses its own challenges for a Westminster which will need to find a new model for its policing relations with the EU after its exit, having previously been a leading contributor to Interpol - whose director since 2009, Rob Wainwright, is a British citizen and former MI5 official.

'Around 40 per cent of Europol casework is thought to have a British focus, and in 2015 UK authorities initiated some 2,500 cases for cross-border investigation,' says Kate Cox, security analyst at RAND Europe, in an interview.

As likely next steps, Theresa May and Home Secretary Amber Rudd will bring forward an expected review of the government's controversial counter-terrorism strategy, Contest, and will propose a substantial expansion of the Prevent counter-radicalisation programme. Only 20 per cent of youths referred to Channel - many of them by schools, universities, and GPs - are assessed after as at risk of violent extremism. A measure of its controversial character is that Baroness Warsi, a former head of the Conservative Party and the first Muslim woman to serve as a UK government minister, in a book published later this month calls Channel 'a textbook example of how to alienate absolutely everybody.'

The EU lacks formalised mechanisms for exchange of intelligence, so Brexit will not impact intelligence sharing. The UK therefore is likely to invest more in Fives Eyes as well as Interpol and the Financial Action Task Force. Britain will accordingly find other tools to replace ones currently within its armory, such as the European Arrest Warrant, Eurojust, the Shengen Information System, and the European Judicial Network. However, notes, Cox, 'this raises concerns about increased fragmentation, administrative costs, and the potential for critical information to "fall between the cracks".'

Losing Britain's current access to Europol, as seems likely, will have significant impacts for both the UK and EU. Similarly, reviewing Prevent and Channel will open controversy about whether the UK approach should be massively expanded, or greatly rethought.

On the other hand, UK security services have according to the Metropolitan Police prevented 13 attempted attacks since June 2013. A terrorist determined to attack Parliament and cause loss of life was only able to obtain a hired SUV and a knife. Though gating policy in Parliament will be changed, and the precise number of firearms officers within the Metropolitan Police will be rethought (it declined by a quarter from 2,856 in 2010 to 2,139 last year), much about the UK approach appears to have a solid record of success (including on 22 March), and a drastic, wholesale rethink of UK counterterrorism policy seems unnecessary and unlikely.

Dr Raveem Ismail
Director, (Re)insurance & Analytcs, Fractal Industries

Comment on the insurance market: We find ourselves in one of the most interesting places in insurance history, at the confluence of what appear to be multiple winds of change:

- At the top of the risk-taking chain, we have capital markets taking an increasing share of what used to be ceded to reinsurers. It is also possible that even should there be, what would have been a market-turning event in times past, that today, it would not increase rates dramatically: it would simply bring the capital waiting in the wings into the open.

- At the bottom of the value chain, we have begun to see, in personal lines, initiatives such as Lemonade, Trov, Bought By Many, etc. Essentially, these are mutualised insurers, enabled by technology, with reinsurance protection, now all dubbed P2P. These aim to disrupt and replace swathes of insurer and broker activity at the bottom of the risk-taking pyramid.

- Throughout, new classes such as cyber, which are heavily non-geographical, do not lend themselves to aggregation using traditional methods. They genuinely require new models for enabling the market to take risk.

Given these, some of what made insurers successful yesterday will not be what allows them to succeed and penetrate new markets tomorrow. It will take a combination of contextual analytical expertise, and a recognition of how there is still a lot of value in producing new solutions rather than fighting for previous relevance, that will allow the industry to continue providing the social purpose for which it exists.

Steve Johnson, MCSFS
Lecturer, Cranfield University, Senior Analyst, Man-Made Risk, Fractal Industries

Comment on terrorism insurance: As an industry we face challenges on a number of fronts in terrorism insurance. On one hand there are the continual challenges of state intervention and market penetration. As we see some evolution in the types of attacks and greater uncertainty in their location, perhaps due to displacement effects, we need to get a wider base taking appropriate insurance. The second set of challenges has always been with us, but has become more pronounced; how do we meaningfully model Business Interruption and even Property Damage when the attacks do not leave classic radial impacts.

Anthony Canale
VP, Crime Analytics & CargoNet, Verisk

Comment on terrorism, and the need to combine insurance with security/continuity solutions: The terror threat continues to be a present danger. The low technology high impact lone wolf attacks in public areas continue to trend upwards. There is no evidence there will be an interruption in the tempo.

Terrorism underwriters and insurers should insure their clients are taking steps to introduce and integrate new technologies and layering the technology into existing physical security groups to maximize their preparedness, planning, practice and response to reduce exposures.

Weimeng Yeo
Principal Modeler, Probabilistic Terrorism Model, RMS

Comment on terrorism insurance relevance, perhaps through capital markets: Despite an increase of catastrophe bonds and other sorts of alternative capital entering the property insurance market, little terrorism risk has been transferred to the capital markets. If terrorism insurance is to remain relevant, it is imperative that they embrace the new tools available to them to create more relevant products, more innovative coverages, and new risk transfer mechanisms that address today's fluid threat landscape.

Adrian Mahieu
CEO, Cortex Insight

Comment on the need for evolution of cyber insurance products and the new regulatory: In relation to regulatory aspects of cyber security, older regimes are currently being augmented with newer more focused requirements. A good example of this can be seen with the GDPR which will become operation as of May 2018 and the changes from the New York Department of Financial Services which introduced stricter regulatory requirements regarding information held on consumers (which was operational as of 1 March 2017). Under the newer regimes the potential fines for non-compliance are massive. Therefore, in my viewpoint, estimating cyber risk is still a dark art. More information is needed to help with setting insurance premiums for cyber risks, the means under which current cyber risk insurance products are priced is unsustainable, and must be changed.

In looking at insurance to cover cyber risks, most insurance companies need a number of data points or previous events to calculate risk, so assessing the risk of someone having a car accident and the costs of that is a science, but being hacked and losing customer data is not. It can take years for a breach and data loss event to be discovered. In this time key staff can change and overall responsibility may be shifted. This is a challenge which insurers must be cognizant of.

Those who engage in cyber security breaches and other forms of cyber attacks use creative techniques. Attackers find all sorts of ways to extract value in all sorts of ways, so that's two unknown variables - unknown risk, and unknown impact/cost. In looking at the bigger problem of how to insure and price the risk, a further difficulty arises in that although most insurance brokers can understand a house fire, or car accident and they can understand most business risk, most insurers still struggle to understand cyber risk.

Lastly, in order to truly improve the cyber insurance market, it is necessary to look at solutions to resolve the lack of data. Currently, there's the problem of data sharing. A company may not be able or care about disclosing they've had a fire at one of their warehouses, so the data globally on warehouse fires is available to input into risk models, but the same is not true for cyber risk. Companies do not like telling the world they've been breached and lost data, so although they sometimes have to come out, many are still swept under the rug. However, the notification requirements within NY DFS cyber regulations and GDPR will change this.

Risk is hard - we filter it by combining with other elements to make it manageable in our product. Insurers need to understand cyber risks and adapt their products accordingly.

Professor Michael Mainelli
Executive Chairman, Z/Yen

Comment on cyber insurance and market growth: Governments see the importance of cyber for national infrastructure security, but much more needs to be done around insurance. Government and business will function much better around a market where insurers are confident they can write realistic and financially viable policies. What can be done is to create insurance for business interruption. Ideally there would be a Cyber Re (reinsurance) pool or club in which the government helps the insurance industry to fund any extreme losses. This is not a radical idea, in 1993 the UK government created Pool Re within the industry covering terrorism for property insurance. Many other governments have catastrophe reinsurance vehicles. From this reinsurance foundation, insurers can write cyber policies around business interruption. It also creates an environment in which the security industry and banks work closely together. Instead of scaremongering, there is an encouragement from all sides to prevent incidents by sharing best practice and collaborating on information. There is much to gain from getting this right. With a fully functioning cyber insurance market, a country would be much more attractive to IT businesses such as financial exchanges and large internet firms.

SHORT ARTICLES

Dr Rachel Anne Carter Managing Director, Carter Insurance Innovations Ltd, Manager & Co-Founder, Journal of Terrorism and Cyber Insurance

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; operating out of London and Paris. Rachel is the terrorism insurance and cyber security insurance subject matter expert for the Security Institute (UK). She is also working as a consultant for the Cambridge University, Judge Business School, Centre for Risk Studies.

Her prior experience working in terrorism insurance and natural disaster insurance includes working for the CEO of Pool Re within a research capacity. Rachel began her terrorism insurance career as an insurance consultant for the OECD in the Directorate for Financial and Enterprise Affairs. 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.

PARIS ONE YEAR ON... RESILIENCE IN THE FACE OF ADVERSITY AND THE NEED FOR GREATER PARTNERSHIP TO PROMOTE CONTINUED RESILIENCE

One year on, there is an eerie silence that fills the somewhat empty streets of Paris. Even the darkness of the evening and the sound of rain on the cobble stones adds to the chill. This time last year changed Paris forever. In 2015, as a result of the coordinated attacks 130 were killed and more than 350 injured, with estimates that up to 600 people are still undergoing treatment for psychological illnesses resulting from the attacks. In the year that followed, in addition to insurance and economic losses (many of the latter from small and medium businesses), there was a drop in tourism, representing a loss of approximately €1 billion. Many of the losses associated with the event and implications for businesses and individuals in the aftermath have not been quantified.

Fear and uncertainty remains a year later in some parts of Paris, because of that frightful day in November. One of the positive implications of the Paris terror attacks was the symbol of hope stemming from greater societal inclusion and candles and flowers that represent love and togetherness are a stronger force that hatred and evil deeds. More importantly, however, the November 13 attacks show that terror events have long lasting and broad implications. The initial shock at the loss of life and numbers of those injured is not forgotten, but it is increasingly becoming evident that there are broader economic impacts that affect communities, businesses and individuals. When looking at the implications from a broader holistic approach, it is important to start to think about solutions which represent means of minimizing loss to life and injuries sustained but also provide financial resilience and economic recovery so that communities, businesses and individuals can bounce back after attacks.

Going forward, there is a role for greater interaction in the fight against terrorism, the different sectors which assist in the aftermath of an event; police, counter terrorist professionals, security professionals, insurers and big business should work together in partnership to promote more holistic results and in doing so where events cannot be prevented, ensuring that there is resilience amongst community and business in the aftermath. France has shown spirit in resilience and the burning desire to honor the key legacy: *liberté, égalité, fraternité* (liberty, equality and fraternity). The joining together of the various stakeholders who can ensure resilience, will in turn promote a safer France, one who can recovery more quickly and a place where tourists should feel safe and welcome.

TRUMP & POTENTIAL RAMIFICATIONS FOR TERRORISM & CYBER INSURANCE

Dr Gordon Woo Catastrophist, RMS**,** Co-Founder & Editor, Journal of Terrorism and Cyber Insurance

Gordon Woo specialises 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.

WHAT IS THE PRICE OF SECURITY?

In 1935, the American Nobel Laureate in literature, Sinclair Lewis, wrote his most important book about USA under the presidency of an outlandish fear-mongering anti-immigrant demagogue. The book, which the New Yorker magazine praised as one of the most important books ever produced in the United States, was entitled, *'It can't happen here'*. Eighty years later, this book is now displayed prominently in bookshop windows. Like Jews living in Europe in the 1930s, many Muslims and Mexicans now living in USA are fearful of losing their civil rights and are threatened by sudden deportation.

'Those who would give up essential liberty, to purchase a little temporary safety, deserve neither liberty nor safety'. According to these words of wisdom of Benjamin Franklin, one of America's Founding Fathers, President Trump deserves to be rebuked for his attempt, within days of assuming office, to suspend entry into the USA of nationals of seven predominantly Muslim countries: Iraq, Syria, Iran, Sudan, Libya, Somalia and Yemen. This firm rebuke has come from the American judiciary, which deemed his executive order to be unconstitutional. All western democracies are exposed, in varying degrees, to a persistent Islamist terrorist threat. Each has to find its own balance between the preservation of civil liberties and the protection of its citizens. Terrorist attacks provoke a change in this balance. Weeks after 9/11, 1200 Muslim and Arab non-citizens were arrested and detained in the USA. 5000 non-citizen men were summoned by the U.S. Department of Justice for interviews. After the 7 July 2005 London Transport bombings, Eliza Manningham-Buller, director-general of the British security service, MI5, warned, *'There needs to be a debate on whether some erosion of civil liberties may be necessary to improve the chances of our citizens not being blown apart as they go about their daily lives'*. On a national scale across America, such a debate took place during the 2016 US presidential election. The female champion of civil liberties and political correctness lost to the alpha-male advocate of tougher counter-terrorism action and profiling of terrorist suspects.

Of all those seeking entry into the USA from the seven designated countries, only a few would have harboured any intent to launch a terrorist attack against their own adopted country. The ratio of immigrants of violent intent to those wishing to live in peace is so minuscule that most western leaders would have baulked at a blanket ban. In 2015, Angela Merkel welcomed into Germany over a million refugees, the majority of whom were Muslim. She accepted the risk that amongst this large multitude of needy displaced persons there might be a number of Jihadists. Germany's refugee obligations under the Geneva Convention outweighed this risk.

However, this is not a risk acceptable to President Trump, who campaigned on a security pledge to make America safe again. It is interesting to note that Trump's core support comes from the interior of the American Heartland which is predominantly less threatened by terrorism than

the East and West coasts which mainly voted for Hillary Clinton. The decision arithmetic on terrorism exclusion policy is an inversion of the decision to rescind President Obama's edict disallowing the sale of guns to the mentally disturbed. A supporter of the National Rifle Association, President Trump has accepted the societal risk that a small number of crazed gun-owners may go on a shooting spree in a public place, resolving not to deprive many others with mental infirmity of their constitutional right to bear arms.

From a terrorism risk perspective, the potential counter-terrorism impact of tightening US border security needs to be assessed. It is well known that Daesh infiltrates its supporters among the hordes of refugees and economic migrants trying to enter Europe. One of the operatives involved in the Paris terror attacks of 13 November 2015 was Ahmad al-Mohammed, a Syrian who arrived in France via the refugee route of Leros in Greece, Macedonia, and Serbia, where he sought asylum on 7 October 2015. Prior to the Paris attacks, the ringleader, Abdelhamid Abbaaoud, made trips between Syria and Brussels. According to the Quilliam Foundation, which monitors radicalization, Daesh pays people-smugglers to bring vulnerable children into Europe. Appalling as it may seem, children of either gender can be groomed for terrorism: in February 2017, a sixteen-year old girl was arrested by the French intelligence agency, DGSI, on suspicion of being a suicide bomber.

Blocking the U.S. entry of a few Jihadis would reduce the threat level in the USA by a small amount. Just as raising the height of river defences around a town shifts the flooding risk down river, so the America First policy of tightening U.S. borders shifts some of the external threat elsewhere. Correspondingly, there would be a small increase in the threat level to American interests in the rest of the world. Extra security may then be needed abroad at American embassies, consulates, corporate offices, restaurants and hotels, including Trump properties.

America's western alliance partners may also be targeted by Jihadis unable to enter the United States. This type of international threat shifting was seen in July 2005, when London transport was attacked by four Jihadis angered by the loss of Muslim lives in Operation Iraqi Freedom. In his martyrdom video, the plot ringleader, Mohammed Saddique Khan, made clear the reasons for the attack. An attack on the Washington DC metro would have been very attractive, but as an Anglo-Pakistani living in Leeds, attacking the London Underground was a less difficult if also less aspirational terrorist operation.

Apart from the external threat, there is also the internal threat from Jihadis already inside the United States. American immigrant families have traditionally been more successfully integrated into western society than their counterparts in Europe, and accordingly less prone to radicalization. Perceiving their President to be an Islamophobe, a few members of the Muslim diaspora, not living the American dream, might be incited by Trump's own rhetoric or tweets to commit acts of terrorism. Any direct attack on the President would be repulsed by very tight personal security. The threat against the President might shift to Trump hotels and his other businesses, or even his close entourage. The most likely attack mode would not be a damaging vehicle bomb causing significant property insurance loss, but rather a lone wolf shooting of the kind that terrorized a nightclub in Orlando on 12 June 2016. Since this shooting, lapses in the psychological testing for Omar Mateen's firearms license have been disclosed. It would be a bitter indictment of Trump's counter-terrorism policy if any future terrorist shooter happened to be one deemed under the Obama administration to be mentally unfit to own a gun.

Tom Johansmeyer AVP, PCS**,** Advisory Board, Journal of Terrorism and Cyber Insurance

Tom Johansmeyer is Assistant Vice President – PCS Strategy and Development at ISO Claims Analytics, a division of Verisk Insurance Solutions. He leads all client- and market-facing activities at PCS, including new market entry, new solution development, and reinsurance/ILS activity. Currently, Tom is spearheading initiatives in global terror, global energy and marine, and regional property-catastrophe loss aggregation. Previously, Tom held insurance industry roles at Guy Carpenter (where he launched the first corporate blog in the reinsurance sector) and Deloitte. He's a veteran of the US Army, where he proudly pushed paper in a personnel position in the late 1990s.

THE CHALLENGE OF CYBER LOSS AGGREGATION

What will it take to help grow the global cyber insurance and reinsurance market? Capacity, of course, makes all the difference. And, the creation of an industry loss index could be a crucial part of the answer. Fundamental to effective ILW trading, an independent loss index could help attract a broader capacity base, facilitating risk transfer at every link in the global risk and capital supply chain. Loss aggregation is an industrywide effort – one that could drive meaningful results quickly for a sector ripe for growth.

Mention cyber risk in the global insurance and reinsurance community, and the reaction may start with some degree of optimism; many see cyber as the new growth class of a generation. It doesn't take long, though, for some flavour of frustration to edge its way into the conversation. This is both understandable and unsurprising.

Called an 'emerging risk', the global insurance and reinsurance industry has had less time to adapt to cyber than it has to property-catastrophe risks. However, cyber exposure is vast, and even though capacity is growing, a 'disaster gap' of sorts remains between capital available and the full set of exposures original insureds have. To accelerate the deployment of capacity worldwide to cyber risks, the market needs access to a new risk-transfer solution set.

The good news is that appetite to underwrite cyber certainly exists. If force of will were the issue, the cyber disaster gap would close considerably. Unfortunately, it takes more than strength of conviction to deploy capital prudently. Cedants and markets need to be able to truly understand the risks they consider assuming, and unless new capabilities come to market, the cyber sector will be constrained by the 'only lay down lines you can afford to lose' approach to risk management.

Of course, modelling will be essential to driving the rapid growth many expect to see in the cyber sector. And there's plenty of innovation in the works and coming to market to help both cedants and capacity providers better understand cyber risk. As with property catastrophe, however, risk-transfer activity stands to become more effective when an independent loss

aggregation solution is available, particularly for the development of a cyber industry loss warranty (ILW) market. With an independent, reliable industry loss estimate for cyber events, it should be easier for a broader range of capital to come to bear on cyber.

In some ways, cyber loss aggregation should be an easy proposition. The same factors that could simplify the process, though, could result in a unique set of challenges. So, what's at stake? Getting loss aggregation right early provides an important tool for global risk bearers when the 'big one' finally occurs. If we wait, our industry once again prepares for a problem that's already occurred.

What Is Loss Aggregation?

While new to the specialty lines insurance market, loss aggregation has been a staple of the property-catastrophe sector for decades—from the formation of PCS® more than 60 years ago, not to mention our legacy organisations that go back even further. Having access to an independent source of industrywide insured loss estimates has facilitated improved underwriting and claims handling in the property space and has helped provide access to a much broader capacity base through industry loss-triggered solutions such as catastrophe bonds and ILWs.

As a process, loss aggregation is fairly straightforward. An independent body, such as PCS, pulls together projected ultimate loss estimates from insurers affected by a particular event and, from there, extrapolates the overall industry impact.

The specialty market differs a bit from property catastrophe. It requires a unique approach, something PCS has investigated over the past few years for energy and marine and other specialty classes. Much of this thinking can be brought to bear on cyber insurance and reinsurance, as well as other classes like terror and energy and marine.

Rather than aggregate a large number of small losses (along with catastrophe-driven commercial losses), cyber and other specialty lines require access to the towers associated with different risk losses. Broad market visibility becomes more important than insight by regional or specific loss market share (unlike the property-catastrophe approach) because a limited number of risk bearers can provide insight into a particular loss.

For cyber, there's an additional factor—the 'cyber catastrophe'. This is a series of coordinated cyber attacks, for example, that result in a collection of related losses across a sector of commercial insureds. Consider the Target breach, but on a broader scale: for example, a Target-sized breach affecting ten companies together in a coordinated attack from the same perpetrator or group (be it formal or loosely affiliated). In such a scenario, the effective aggregation of the loss would involve the PCS approach to specialty markets (such as marine), in which the number of insurers affected is smaller. It would also include elements of how we approach property catastrophe, in that there would be broader, market wide implications, with the number of insurers affected increasing because of the number of individual risk losses from the event. In the end, the risk losses would have to be aggregated into an overall loss—as long as it's possible to trace the activity directly back to a common source.

Ultimately, loss aggregation activities enable the creation of a central repository of industrywide insured loss estimates and relevant descriptive information to support deeper risk understanding and industry impact, which can be an important prerequisite to increased ILW

trading. Constructing a loss aggregation methodology, however, relies on the availability of historical losses; and for the cyber sector, the number of events that would be relevant for inclusion in a historical loss database is even smaller than you'd find in terror.

Why Do Historical Losses Matter?

Part of the process for developing a loss aggregation methodology is to review potentially relevant previous incidents and their attendant losses. Past events can provide important indicators that inform such decisions as where to set the industry loss threshold for what qualifies for investigation under a loss aggregation scheme.

Based on research conducted jointly by PCS and Sciemus, two events have occurred in the past five years that have resulted in insured losses of at least around $100 million industrywide, although the losses for a few others appear to be developing still (Yahoo and Dyn, for example). To move to a lower threshold would be to dive to a level too granular to be relevant for most reinsurance and retrocessional risk transfer. One could even say US$100 million is pretty low. However, given that we've yet to see the industry-defining 'Cyber Andrew' event, our community is left to speculate as to what would constitute a sufficiently significant loss for reinsurance risk transfer.

To give you a sense of the state of infancy of cyber insurance and reinsurance, consider what US$100 million means in the U.S. property-catastrophe market. In 2016, 37 catastrophe events (some subject to resurvey by PCS) had industry losses of at least US$100 million. Meanwhile, US$100 million in insured losses for a cyber event is noteworthy.

With this in mind, historical losses provide little insight into what the true 'cyber disaster' scenarios could be. Ascertaining what a Cyber Andrew–type event would look like remains an exposure-based effort absent a sense of actual losses. That said, a loss aggregation solution could still facilitate risk transfer—especially to the capital markets—based on a cedant's understanding of its exposure. The determination of trigger points will simply remain a work in progress until the big one occurs.

So, What Do We Get?

Loss aggregation is truly an industrywide effort, something we see every day at PCS. In addition to the work our team conducts, we fully understand that the companies supplying loss information invest in the process—through their time and usually when they are busiest. The benefits of participation, therefore, need to be significant. And cyber is likely to become a textbook case of the difference that loss aggregation can make.

Perhaps most important is the potential for a loss aggregation solution to help attract capacity to the cyber market. Right now, most cyber coverage is limited in both size and conditions. Much is excluded, with restrictions that ultimately result in eroded cover that provides little of the protection original insureds actually need. With broader sources of capacity that are better able to understand the risks they may assume, cyber writers may be able to provide more relevant protection to their clients. This would ultimately drive a much larger and more robust market, providing meaningful cover in an area that has frustrated our industry for quite some time.

As an industry, we've gotten started on cyber—but that's about it. We have a long way to go,

and effective loss aggregation may provide an important lever for us in the maturation process.

Spike Townsend GCGI LCGI Director, STRaR Ltd

Spike is the co-founder of STRaR Ltd, the only UK commercial company currently with permission to implement the UK Crowded Places Protective Security Improvement Activity (PSIA) tool outside of Counter Terrorism Policing. Previously, he was a police officer of nearly 30 years' service, the last 14 as a UK counterterrorism protective security specialist. He is a trained counterterrorism security advisor (CTSA). His experience includes 3 years working on the 2012 Olympic Games as a CT protective security advisor to LOCOG, the CT design advisor for the Westfield Stratford shopping centre build and the UK Crowded Places desk officer at the National Counter Terrorism Security Office (NaCTSO) where he was jointly responsible for the development and delivery of the PSIA tool and 2014 CONTEST UK Crowded Places program.

CAN INSURANCE FURTHER DEFINE TERRORISM RISK MANAGEMENT & LOSS MITIGATION CREDIT (LMC)?

Should the Insurance industry be doing more to incentivise security benefits in respect of terrorism property and Business Interruption Insurance.

Terrorism and violent extremism are a continuous and sustained threat to the United Kingdom and beyond. In recent years this threat has evolved with new attack methodologies and ideology either directly tasked or inspired that has led to an increase in both the scale and intensity of atrocities. The indiscriminate nature of the contemporary terrorist threat, its pace, ferocity and scale of multiple coordinated attacks has and continues to be a significant challenge for all those operating within the terrorism landscape, whether commercial or public. The threat vector to the UK is very real, evolving and difficult to counter in isolation without well thought out, proportionate and cost effective initiatives to encourage dialogue and counter terrorism (CT) protective security improvement activity. Whilst the Government counter terrorism strategy requires UK CT Policing to undertake and report on activity and to demonstrate how "crowded places" are better protected, there are inhibitors to wider UK coverage which the insurance industry could support.

The UK security machinery has and continues to rely on public engagement and business interaction to ameliorate the threat. Given that the first rule of government is to safeguard its citizens, it could be argued that the public sector [law enforcement and HMG departments] have not adequately explored [in a counter terrorism context] the use of Public Private Partnerships [PPP] within the CT space to provide "real world" cost effective and proportionate mitigation measures with a scalable financial premium discount. For the wide ranging purchasers of terrorism insurance [Small Medium Enterprise [SME] to multi-nationals], the drivers are significantly different, yet the desire to apply CT protective security principles remain relevant.

The application of a PPP "insurance driven" terrorism risk management [premium] Loss

Mitigation Credit (LMC) model, rewarding participation in a national counter terrorism protective security model via a premium discount, additionally reflects a better rated risk for the insurers. Although reflecting low probability-high impact event[s], a consistent, inclusive and intuitive model that applies to not only crowded places but also the wider terrorism market, may be demanded of insurers. However, the Insurance industry itself, playing a vital partnership role can also take a lead.

By way of example the LMC offered by Pool Reinsurance (Pool Re) for businesses participating in the UK Governments crowded places program offers its members a 2.5% discount if they undertake the Protective Security Improvement Activity (PSIA) tool. This scheme is currently limited to those sites or organisations that have been previously identified by NaCTSO and who are currently participating in the scheme.

Another option is the provision of innovation funding via access to Risk Improvement Funds that can be applied to terrorism property insurance. Funding is provided by the broker to the client so the client can undertake assessment and action plan security improvements. This assessment could include the PSIA or any other auditable improvement tool. This funding innovation is available thru a limited number of brokers and is currently providing added value to clients, but equally as important, is allowing its clients to make tangible difference to business terrorism protection. Industry innovation, product differentiation and price will continue to support client retentions and attract new SME business in a soft market.

The ability and provision of protecting the UK and its business assets is not solely reliant on HMG or UK policing. The businesses themselves have a responsibility to not only protect, but to review, and identify improvements to their security regimes against terrorism attack methodologies, in a proportionate and consistent manner. Making UK PLC safer and more resilient can be enhanced if the insurance industry, especially in respect to Property and Business Interruption insurance, can look to reward those clients that take protective security improvement activity seriously. This can be achieved either by providing innovation funding at the front end or LMC at the underwriter position.

LONG ARTICLES

Desmond McCormack, CEng FIChemE Head of Risk Engineering Services, RKH Specialty

Desmond McCormack is a Chartered Engineer and a Fellow of the Institute Of Chemical Engineers. He has extensive experience of providing consultancy services in aspects of risk engineering and management across a wide range of industries including oil and gas, power, mining, petrochemical and chemical, pharmaceutical, steelmaking, transportation, food and retail.

William Horner, MBA CEng Managing Director, Horner Technology

William Horner is an independent consultant specialising in the security of industrial automation and control systems. He has been working on industrial cyber security since 2003, was the global technical lead for a major chemical company and authored the security guidelines actively used across several hundred chemical plants.

Jerry Smith, OBE Managing Director, Ramehead Consulting

Jerry Smith, OBE is an independent security risk management consultant, specialising in CBRNE threat management. He has over 25 years' experience of global security risk management within Bomb-Disposal, Counter-Terrorism, Humanitarian De-mining and WMD Counter Proliferation.

ON-SITE RISK SURVEYS WITH AN ALIGNED APPROACH FOR PHYSICAL AND CYBER SECURITY TO REDUCE THE POTENTIAL EXPOSURE FROM CYBER- ATTACKS ON INDUSTRIAL CONTROL SYSTEMS

The rise of connectivity in all aspects of business activity is resulting in significant capability and efficiency improvements; none more so than in the field of digitised industrial control systems (ICS). But with these developments comes the potential for cyber-related threats.

The internet has long been used as a platform for the communication and organisation of illegal activities. With the advent of big data, personal and financial information became the target for disturbance and theft. The focus of concern is now shifting toward a third level; that of data manipulation to influence and control these industrial systems. This emerging threat has the

potential to result in actual physical disruption to occur; with the resultant risk of property damage, business interruption and loss of life.

Three common misconceptions are identified. Firstly, ICS are isolated from on-line administrative networks, secondly that such systems can only be accessed remotely for maintenance purposes and thirdly, that systems receive, rather than transmit, data and instructions.

ICS are not only vulnerable from networked attacks. The very nature of ICS means that it is not always possible to replicate secure centralised servers. So the physical protection is vital element in a risk mitigation strategy.

In conclusion, the effective assessment of security risk to ICS requires an integrated systems approach; surveying both the physical and cyber domains to ensure vulnerabilities are identified and mitigated.

Introduction

Whilst the majority of recent discussion concerning cyber risk has concentrated on the potential to cause non-physical damage to digital assets, by the theft or corruption of data, or a denial of service, there has been growing concern about how such an attack could extend to cause damage to physical assets.

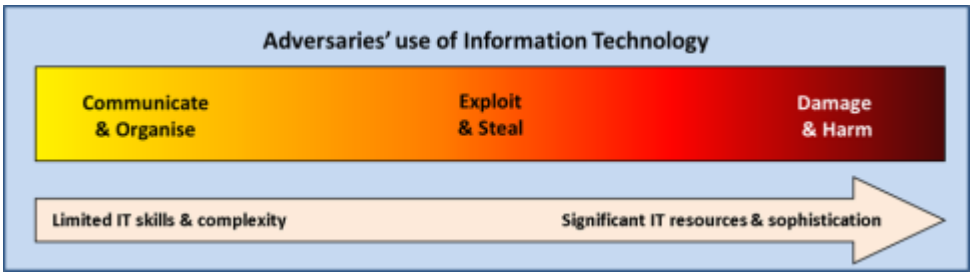

Figure 1. The spectrum of information technology threats

This is a concern for large manufacturing plants which employ increasingly sophisticated industrial control systems to optimise the performance of, and safeguard, equipment. Indeed, our observations while undertaking risk surveys at such sites is that many operators are currently undertaking, on their own initiative, various types of stress testing to identify potential vulnerabilities between their Information Technology (IT) and Operation Technology (OT) systems. (Note that in this paper when referring to IT and OT that we will use the definitions which are attributed to Garner Company whereby IT refers to the entire spectrum of technologies for information processing, including software, hardware, communications technologies and related services. In general, IT does not include embedded technologies that do not generate data for enterprise use. OT is considered to be hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise.)

Our conversations with risk managers has highlighted to us that most companies these days are experiencing, on a frequent basis, some type of attack on their IT systems and that risk

managers are naturally concerned about the potential consequences should such attacks have an impact on their companies OT systems.

Mitigating such risks through insurance is a major challenge not just for risk managers but also for underwriters who are being asked to provide various types of cyber cover to indemnify against the losses resulting from an attack. A particular challenge for underwriters is the availability of sufficient information to assess the potential exposure.

In addition to their own research a common way to obtain more information is by commissioning an on-site risk survey by a suitably experienced risk surveyor, and through a risk survey report the observations of the surveyor can be shared with the underwriters.

This presents the challenge of assessing the complexities of the risks from cyber-attacks on an industrial plant to the risk surveyor who when faced with the task of obtaining the relevant information must review the methods they use for collecting and analysing information on a 'normal' risk survey and consider whether these can be applied, whether they can be modified, or whether new methods need to be developed.

Our solution has been to develop an approach that is based on existing methods but with some modifications so as to allow us apply a range of different skill sets, provided by surveyors with different specialisations.

The methods we have adapted are based primarily on our approach for undertaking risk surveys to support Terrorism and Political Violence programmes. Such insurance programmes are used to provide coverage for property damage and business interruption resulting from events such as terrorism and sabotage, strikes, riots, civil commotion, malicious damage, insurrection, revolution, coup d'état, war and civil war.

The advantage using such methods is that if one considers the nature of cyber risks then, similar to the threats from terrorism and political violence, cyber threats will generally originate from outside the boundary fence. For such risks one has to acknowledge that while plant site operators may be able to manage and control activities within the site perimeter they are not able to exert such influence over the activities of potential adversaries who are operating outside of the site. An important exception to this is what might be referred to as an insider threat, arising from a disgruntled employee, but this is not ignored in our approach.

International and domestic adversaries

An example of one of the modifications that we have had to consider in adjusting our approach is to account for the different ways in which threats can be delivered. When considering cyber risks, there are two key pieces of guidance to keep in mind:

1. Cyber threats do not respect traditional physical, geographical or national boundaries. The existence of a network connection or the movement of media and equipment through these traditional boundaries is often sufficient on its own to facilitate the free movement of cyber threats.
2. An adversary with sufficient physical access can override most (if not all) layers of cyber protection.

Whilst a conventional terrorist threat normally requires physical assets to be deployed at or in the vicinity of the plant site, a cyber threat can be delivered both locally or remotely, from thousands of kilometres away and with little physical risk to the attacker. For this reason, it is necessary to coordinate both physical and cyber security approaches under a single aligned risk management strategy.

Therefore, our assessment of the capabilities and intents of potential adversaries needs to be more extensive. Normally our assessment of potential adversaries is limited to those who have or may gain physical access to the site and includes four main groups - criminal, terrorist, local communities and employees, however when considering cyber threats our assessment of potential adversaries includes sub-categories for those adversaries with similar goals, but have the ability to cause effect via access through IT systems. Therefore, given the current global nature of criminal, terrorist and community groups it is necessary to analyse them from both a domestic and international context.

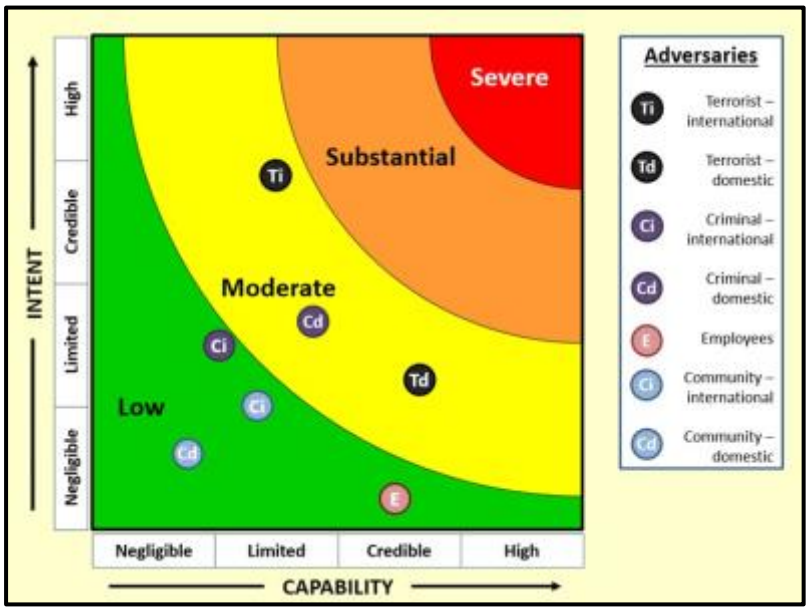

Figure 2. Assessing the capability and intent of potential adversaries

Our approach also includes an assessment of the countermeasures that are currently in place to prevent and reduce the impact of an attack. In assessing countermeasures, the key criteria, we are considering is whether they are appropriate considering the threat, not necessarily are these the best possible countermeasures available.

In addition, we consider the potential impact of an attack, whether there are specific features of the plant that increase the possibilities of an attack being successful and are there specific features that would increase the severity of a successful attack. When conducting such an assessment on behalf of underwriters then severity is usually quantified in terms of financial losses caused by damage to physical assets.

An important part of the survey is providing recommendations and although we normally draw on our own experience to provide these it worth highlighting that there are several good references available from open-sources that provide guidance on current good practises, the document *Cyber Security Assessments of Industrial Control Systems* published by the Centre of the Protection of National Infrastructure is such an example.

To illustrate how our methods for risk assessment methods can be applied we will continue with the analysis of adversaries and consider one of the important aspects of cyber threats which is how vulnerabilities may be created that these adversaries may seek to identify and may subsequently exploit.

The interface between Industrial Control Systems and the rest of the business

Most experts will advise us how these industrial automation networks are in reality becoming increasingly connected and interconnected. However, this trend is not new and has been going on for many years. Any of the following can apply strong business drivers to establish some form of data connectivity with the industrial automation/control systems:

- Tax, accounting and auditing processes requiring production volumes or warehouse inventories (to be accurately measured and reported or recorded)
- Environmental laws requiring the collection and long term archival of accurate laboratory and process data. Automated and specialist analysis equipment is sometimes also required to support this.
- Monitoring services that deliver real time production data directly from the industrial systems (such as machine performance or chemical analysis results) to Specialists located at remote central 24hr manned control rooms.
- Vendor support contracts requiring direct data connectivity from their offices to the industrial automation systems in return for faster response times or a contract price discount

It is at these interfaces that vulnerabilities can exist which can be exploited and in our experience there are three common misconceptions and failures when interfacing the industrial control systems to the rest of the business. The first stems out of the following common management statement:

> *"Our industrial automation systems are completely isolated. They are not connected to the IT networks."*

In their defence, the automation systems were probably procured independently from the rest of the company networks and may be managed by different teams. And the network cables might not be directly connected and are probably not integrated. Unfortunately, the technical awareness still needs to be improved in many of these situations. For example, having a personal computer or server connected to two different networks does not isolate (or "air-gap") the networks. Quite the opposite in practice. And even the best firewall or diode can provide minimal to no protection unless it forms an integral part of a larger, carefully engineered security design. For example, it is relatively common to find that the sensitive internal automation networks are extending outside of the relatively secure physical confines of the inner plant boundary fences to remote IT rooms.

The second common misconception is that many people focus on industrial automation systems by taking a maintenance support view to security. "Remote access" for many means being able to share screens, share files and even take remote control of keyboards and mice. There is certainly a fair amount of such practices taking place on industrial control systems and to a large extent, mainstream IT security practices and solutions can and do help in this respect however this is not the only way an industrial control system can be remotely accessed.

And this brings us to the third area. Where the industrial control system security starts to differ from the mainstream IT security knowledge is at the data interfaces, where deterministic and predicable performance is highly desirable a lot of engineering effort is put in to removing potential failure modes at source. In response to the above, common business policy statements for industrial control systems, often make statements similar to the following:

> *"It is not possible to remotely modify parameters on the industrial automation system. We only push data out from the plant. The plant data historian is read-only."*

At face value, this statement looks strong and good for industrial control system security but in reality may not be implemented as such in practice. Some basic additional knowledge can provide tremendous help with the security. Common situations that can result in unintended risk exposure despite physical and cyber protection measures are presented here:

1. Industrial Automation Open Platform Communications (OPC) servers

Many enterprise historians or Manufacturing Execution Systems (MES) will use the OPC data protocol as the primary data interface. Some will talk OPC directly over the network. OPC has a reputation of being problematic when used over Ethernet so some vendors solve this by using their own bespoke network protocols to connect to their own interface software running on the same server as the OPC interface itself. Either way, standard OPC is probably being used somewhere in order to supply external enterprise historians with production data.

The single best place to ensure that data can only be read (read-only) from the industrial automation system is on the OPC interface itself and industrial automation systems usually provide at least some options to configure the OPC interfaces.

On some systems read/write permissions are a global option i.e. all interfaces are read/write or all interfaces are read-only. It is less common to be able to define read/write permissions for specific interfaces and at the time of writing it is still rare to be able to define read/write permissions based on the data itself.

The issue is that industrial control systems also use these same data interfaces to connect together multiple internal systems, not just provide data to remote systems such as enterprise historians. Applications might include two-way data interfaces to third party control systems on turnkey skids, sharing data with logistics facilities and even interfacing to the safety systems.

Therefore, it is quite common to find that by design the industrial control system will allow any connected system full read/write access to most (if not all) process variables and set points. That is how they are designed to operate. So the OPC interfaces are rarely designed to apply the standard IT concepts of data permissions and confidentiality.

The basic assumption should be to assume that anyone with an OPC data connection can write, modify and control any parameter on the industrial automation system. If in doubt this is simple to test without posing any serious threat to the control system by using some temporary data points. No specialist penetration testing skills are required.

2. Historian data collection

As will now be apparent, when people refer to the plant data historian as being "read-only", they are usually referring to the fact that the plant data historian is only configured to read data. However, the plant data historian can also be configured to write data to the industrial control system and that configuration sits on the plant data historian itself. There are many genuine situations where this is actually quite useful, such as for MES, batch and recipe control. Even a simple data watchdog to confirm that external systems are recording critical environmental variables would require some form of write access back to the industrial control system.

It is also common to find industrial control systems implement a layer of data processing to ensure that any data that has been provided from an external system is good before the industrial control system takes the defined actions on it. This helps to protect the control system from well-known (non-malicious) threats such as simple software bugs and network failures. However, this data processing is usually only implemented on the specific areas that intended to be written to from external systems. Not all the other internal data variables.

So who has been given enough permissions and privileges to be able to reconfigure the plant data historian? Who do they work for? And where are they located? This individual in practice may already have sufficient access to take remote control of the industrial control system, even though that might not be the intended design nor the accepted working practices. At the simplest level, the first place to look at is who holds the server administrator privileges for the plant historian. And second, who holds sufficient privileges to set the server administrator privileges. These are areas where business requirements, risk awareness and a fully engineered technical design are required. Simple management statements such as "this team manages all servers in this company" may be a best practice in service management, but it may also be indirectly undermining the security of your industrial control system and exposing the business to risks that have already been stated as unacceptable in the business policies.

Local access and physical security

Although the previous discussion has focused on vulnerabilities that an adversary can exploit remotely – that is from outside of designated local physical areas or zones, we must also consider those who may seek or may even have been granted access to such areas, for example employees. The potential impact of such adversaries cannot be underestimated, and one of the reasons we use a multi-discipline team for such risk assessments is to review certain aspects of physical security at the site.

Physical access will provide the opportunity to by-pass electronic countermeasures such as firewalls. This is most likely to be in the form of human involvement; either through error, or most commonly incorrectly followed processes and procedures. If storage devices containing sensitive data are not in a physically secure location then they can be stolen whether the data is encrypted or not, and if the (cryptographic) keys are stolen or broken then the data on the device becomes exposed. An example of such an incident is the Stuxnet worm which it is believed was introduced to its target environment via an infected USB flash drive.

Remote facilities and physical security

A final example of how the scope of the risk survey becomes more extensive is that when we discuss local access to a facility that we normally consider local to be an area of the site or its operations that is directly under the operators control or 'inside the fence', however when considering operations such as pipelines then this can also include associated facilities such as

compressor, pumping or block valve stations, which will inevitably be some distance from the supply and receiving stations.

However, controlling the physical access to these associated facilities, to the same level that the access to the supply and receiving stations can be controlled, is not normally practical and an area where vulnerabilities to the supervisory computers for such operations can arise is through the communications from the instruments installed at these stations.

It is increasingly common for such stations to be installed with sophisticated field instruments as part of a supervisory control and data acquisition (SCADA) system as such a system can provide many advantages in managing pipeline operations.

In a similar way to the previously mentioned sensitive automation networks being extended outside their plant boundaries, systems like SCADA rely on communications such as satellite channels, microwave links, or cellular phone connections to relay field data and an area where we have seen vulnerabilities arise is through weaknesses in the verification procedure to confirm the identity of operators communicating through such channels. Even if the supervisory computers for the SCADA system, and any networks that they are connected to, are protected by comprehensive physical security measures then these can be by-passed if the communication channels transmitting data to them can be accessed.

Conclusion

Assessing the level of exposure from potential cyber exposures can be very complex exercise and when attempting to make such an assessment then underwriters will best be supported by access to reliable and credible information. Commissioning a risk survey can provide access to such information and in our experience a survey of this type can be most effectively done using multi-discipline teams.

In this article we have highlighted only one aspect of the many threat factors that need to be considered but already this distinction between groups of international and domestic adversaries illustrates the additional levels of complexity that can exist.

An additional challenge for both underwriters and surveyors is that cyber threats are continually evolving and security measures can become quickly outdated. The schematic shown in Figure 1 only reflects an assessment of the capabilities and intents of potential adversaries at a particular point in time, and as experience has shown a modest increase in an adversary's level of intent can be accompanied by a significant and disproportionate increase in capability if easy access to resources such as financing are available.

Access to new technology is also something that many industrial plants are seeking to exploit and this is driving a demand for more information to support improvements in operational performance, it is anticipated that the number and type of connected devices in plants will increase. Wireless communications and virtualisation add additional layers of complexity and so new vulnerabilities will be introduced. Nevertheless, our experience has also highlighted to us that many plants are increasingly aware of potential vulnerabilities and those that might be considered best-in-class in this regards are pro-actively testing their information and operational technology systems to identify such vulnerabilities.

On-site risk surveys can provide support to support plant operations by providing recommendations based on the surveyor's experience of best practises in the industry and we have seen that in many cases there are 'low-hanging fruit', and that with relatively modest efforts that the most obvious vulnerabilities can be quickly addressed.

Industrial Control Systems

An industrial control system (ICS) is integrated hardware and software designed to monitor and control the operation of machinery and associated devices in industrial environments.

Industrial control systems monitor, automatically manage and enable human control of industrial processes such as product distribution, handling and production. ICS are used in extraction resources like mining, oil, gas and coal, as well as factories, water/waste water treatment, power plants, pulp and paper and transport industries. The systems have helped bring about an increase in speed, responsiveness to conditions and reliability.

Technologies used in ICS include distributed control systems (DCS), programmable logic controllers (PLC) and supervisory control and data acquisition (SCADA). The separation of these systems is becoming less defined as remote telemetry units used to input change become more capable of local control and information technologies (IT) are increasingly integrated with operational technologies (OT).

Historically, ICS hardware was not networked. Many devices for monitoring or adjustment had no computing resources and those that were computerized typically used proprietary protocols and programmable logic controllers rather than full computer control. However, a major focus of the burgeoning Internet of Things (IoT) – and the Industrial IoT in particular – is networking non-computing devices and making it possible for them to exchange data over the Internet.

Despite the benefits of OT modernization and IT/OT convergence, there are drawbacks in terms of security. The modernization efforts often expose older, previously unconnected and harder- to-update systems to new threats. As a result, previously secure facilities may be left open to industrial espionage and sabotage. Kaspersky Labs defines targeted attacks against ICS as the number one threat to critical national infrastructure.

http://whatis.techtarget.com/definition/industrial-control-system-ICS. Accessed 19th October 2016.

Clive O'Connell Partner & Head of Insurance & Reinsurance, McCarthy Denning

Clive O'Connell has practiced as a lawyer in the insurance and reinsurance market for the past 35 years. He is currently the head of the insurance and reinsurance team at McCarthy Denning. He is also a non executive director of Twelve Capital UK Limited as well as being General Counsel and a board member of the International Insurance Society.

DEFINING TERRORISM AND TERRORIST RISK FOR INSURANCE PURPOSES

Terrorism is a difficult term to define and many attempts have been made to define it for political purposes. These definitions change as the political landscape changes. Insurance requires a definition of terrorism that withstands political movement. Consistent definitions allow insurers and insurers certainty. Rather than creating bespoke definitions, parties to insurance transactions are advised to accept definitions used across the market.

The question of the definition of terrorism is a fraught one. It has significant political ramifications.

The importance to the insurance industry surrounds the existence of separate terrorism cover and government backed terrorism pools as well as the terrorism exclusions required in other products to allow the two covers to work efficiently together.

A problem with terrorism is that it is created in the minds of humans to influence the behaviour of other humans. As such it is as infinite in its manifestations as the human imagination will allow.

Natural catastrophes are easier to define. We know what an earthquake is and can define a hurricane by its geographical originals and its wind speeds. We have also had experience over many years to understand the significance of fire following earthquake and the difference between flooding caused by rain and tidal surge. Wordings have developed over the decades to deal with the nuances of such claims.

Among man made disorders, riots and civil commotions, wars and insurrections have been round for long enough to allow for judicial definition which gives allows for confidence among draftsmen when using those words that they will be understood and interpreted as they were intended.

Terrorism is more problematic. Of course, terrorism has been round for a long time but until the IRA “spectaculars” in the City of London in the early 1990s the insurance implications were not separate from other losses.

The two major bombings in the early 1990s created a major concern for the British Government. While security in the City of London was increased significantly and the Ring of Steel created, concern still existed as to the ability of the insurance market to cover a very large attack. The aim of the IRA had become economic rather than simply to terrorise people.

The solution was Pool Re and, for the first time it became necessary to distinguish between what was a terrorist caused loss and any other type of loss.

Since the 1990s, the need for terrorism cover separate from the general body of insurance cover has increased as the threat from terrorism around the world has increased. The way in which terrorist attacks are made has developed. The need exists for a definition of terrorism that encompasses everything that is terrorism and excludes everything that is not.

Of course, that is easily said. One only has to look at the political debate that occurs after every atrocity to see that it is not so easily achieved.

A gunman walking into a government building, a night club, a church, a mosque or a college and killing people, will be described by some as a terrorist and by others as insane, depending, often, on their own political or religious affiliation. Participation in political internet forums or possession of a Quran does not make mentally ill people any less mentally ill. At the same time, it could be argued, few sane people take to terrorism.

Defining exactly what is terrorism and what is not is, accordingly, difficult for political purposes and for insurance purposes. The difference is that grey areas are allowed in politics but have no place in precisely drawn insurance and reinsurance contracts. It is essential to define terms so that they can be known and understood and so that, once an event occurs, all concerned can know immediately what exposures exist and what recoveries can be made.

A similar issue has beset the insurance and reinsurance markets in seeking to determine which losses can be aggregated together into one claim when they arise out of similar circumstances or appear to have a common cause.

Two significant examples of this conundrum exist in the sphere of terrorist related losses with the Black September Dawson's Field events of 1970 and the 9/11 attacks in 2001.

In both cases the question arose as to whether multiple hijackings which appeared to have been coordinated gave rise to one aggregate loss or to multiple losses.

Insurance and reinsurance draftsmen have struggled with the definition of "event" or "originating cause" or "occurrence" or similar language for a very long time.

In the London Market there were a number of cases that went to appeal from arbitration decisions on what constituted one event. Although the definition given by the courts left some people upset by the consequences on the claims that they were making or the payments that they had to make, the consequence of these decisions was that everyone now has a clear idea of what the most frequently used clauses actually mean.

Insurance and reinsurance are concerned with unknown future events. Some of these events are "unknown unknows". It is impossible to predict what a future claims scenario might throw up. That said, because we have some clarity from the courts as to how they will interpret the most usual event wordings, those wordings can be used with confidence that it will be possible to apply the same method of interpretation to future unique or novel claims situations. The cases provide a template if not an answer.

For this reason, most reinsureds and reinsurers will use the words:

> "each and every loss and/or occurrence and/or catastrophe and/or disaster and/or calamity and/or series of losses and/or occurrences and/or catastrophes and/or disasters and/or calamities arising out of one event."

There have been some, over time, who felt that they can improve on those words. There are perhaps some brokers who, in a soft market, feel that they can obtain a better deal for their clients. They seek to use other words. In doing so they inject a new risk into the equation.

It took many years and a considerable amount of money to obtain the court decisions which define the most usual words. These words may not be ideal. The deal with abstract future events at the time in which they are inserted into contracts. No one knows the claims to which they will be called upon to respond. Once the claims do arise, they do provide a guide as to how those claims should be aggregated.

Clever new wordings however, do not provide that same guide. While new wordings may be felt by their draftsmen to cover potential future scenarios more effectively, they are untested. Novel claims scenarios could place unexpected strains upon them; strains that give rise to disputes.

It is generally better to adopt and accept widely used wordings which have been tested before the courts. One has a better idea of how they will respond and, because they are widely used, it is more likely that, even in the most complex situations, dispute can be avoided or, if there is a dispute, one will sit alongside the rest of the market in it.

A unique and novel wording, which is untested, however, runs the risk of an isolated challenge. This rule, which applies as much to terrorism covers as to all other covers, also applies to definitions of terrorism.

The courts have not yet had to struggle with a definition of terrorism and so, the wordings created over the past 25 or so years do not have the robustness that one might desire and which comes from challenge and determination. That said, there are definitions now in common use. To this end, the following definitions produced by the LMA are useful:

> "an act of terrorism means an act, including but not limited to the use of force or violence and/or the threat thereof, of any person or group(s) of persons, whether acting alone or on behalf of or in connection with any organization(s) or government(s), committed for political, religious, ideological or similar purposes including the intention to influence any government and/or to put the public, or any section of the public, in fear."

Or

> "Act of Terrorism means an act or series of acts, including the use of force or violence, of any person or group(s) of persons, whether acting alone or on behalf of or in connection with any organisation(s), committed for political, religious or ideological purposes including the intention to influence any government and/or to put the public in fear for such purposes."

Using such definitions allows one the knowledge that other participants in the market will face exactly the same questions at the time that the loss occurs. Reinsurers are as likely to interpret the contract in the same way due to other involvements.

To put it another way, if a flaw is found in the wording, one will not be alone in dealing with that flaw and one could benefit by a market wide compromise. To go alone and seek a unique solution to the definition exposes one to the possibility of dealing with one's own flaws alone. There are areas in which to create unique advantages in selling or buying insurance and reinsurance; terrorism definitions is not one of them.

When using any clauses, one should also be aware of one factor that might mean that even a standard clause is susceptible to a variety of interpretations. The choice of law and jurisdiction that is applied to a contract can have a very real bearing on how it is interpreted.

Sadly, we will continue to see new terrorism events and as terrorists become more inventive to avoid security and detection, there will be attacks that challenge any interpretation and wording. Those challenges are best faced standing together with the rest of the market rather than alone.

Dan Kaszeta Managing Director, Strongpoint Security

Dan Kaszeta is an independent consultant in chemical, biological, and radiological defence and various security disciplines, currently based in London. His 25-year career spans service in the US Army, the White House Military Office, and the US Secret Service, before switching to the private sector in 2008. He is the author of *CBRN and Hazmat Incidents at Major Public Events* (Wiley, 2012) and the author of numerous articles.

PROTECTING AGAINST CHEMICAL AND BIOLOGICAL RISKS TO OFFICE BUILDINGS

The risk of chemical and biological incidents to office buildings is very difficult to estimate or model. Releases external to a building vary quite differently from releases internally in a building. However, for any given set of incident parameters, there are defensive measures which can be implemented. While every building is different, there are some overarching principles which can guide building design, retrofits, and emergency planning. There are also certain specific measures which are known to have value in preventing damage, deterring hostile acts, or mitigating the damage from incidents. Many of these measures involve ventilation and air conditioning systems, while others are more procedural in nature.

Chemical and biological (C/B) threats to office buildings remain thankfully rare. Concrete examples are few. Likelihood of harm is difficult to grasp in the abstract, and modelling of this type of risk is quite difficult. However, some mitigation techniques and practical defensive measures that have a high likelihood of preventing harm from happening, reducing harm when it happens, or restricting the spread of harm. The purpose of this article is to provide sound guidance on measures that owners and occupiers of office buildings, both public and private. While the suggestions in this article have been developed with office buildings in mind, they may have applicability to other premises. Additionally, the primary threats addressed here are chemical and biological substances and this article does not specifically address radiological threat even some aspects of the radiological threat may also be mitigated by some of the suggested measures.

Providing a high degree of protection for a broad spectrum of chemical and biological threats

for normal office buildings is generally considered prohibitively expensive. A very large array of measures, many of which would range into the millions of dollars per building or large amounts of skilled labour, are required to obtain a degree of protection that would obviate the threat. Some measures have high value, but if performed in a flawed manner actually make some aspects of the threat worse. Skills in this area are rare and the work required is sophisticated. This degree of effort and expense is unlikely to occur except at the most important parts of national infrastructure, such as parliaments and military headquarters. However, there are a wide variety of measures that provide some degree of partial effectiveness that may serve to deter hostile acts, provide partial protection, or mitigate the impact of an incident by reducing the extent of damage. Some of these measures are low cost and/or provide ancillary benefits in traditional physical security and crime prevention.

This article is divided into two parts. The first part describes general principles that need to be understood in order to seriously mitigate the threat from C/B threats. The second part describes some specific measures that can be applied. Not every specific measure described in this article is applicable to every situation and location.

General Principles

Location of the threat

When talking about C/B threats to buildings, it is useful to divide the threat into two categories. External releases are some sort of dissemination of a threat substance outside the building. Example scenarios would be an accident involving a truck or rail accident involving commercial industrial chemicals upwind of the target site, or a terrorist device located outside the building, or an incident in an adjacent building. Internal releases are situations where the C/B threat is dispersed inside the building. An example scenario would be a package with a hazardous substance that is opened in a mailroom or at someone's desk. Part of the complexity of dealing C/B threats derives from the fact that some measures against external threats may make internal threats more dangerous or vice versa. It is also worth considering "insider threat" – the possibility that an employee may be the initiator of an incident.

Physical Characteristics of the Threat

Threats may come in solid, liquid, gas/vapour, or aerosol form. Aerosols are a finely divided mist of either solid or liquid matter. While a comprehensive catalogue of threat substances is beyond the scope of this article, a few simplified assumptions can be made. For chemical threats, the most likely external release is some substance that has travelled a distance to get to the target building. Generally, this would be a gas or vapour, or an aerosol. Internal releases could be liquid released from some sort of package or container, which may in turn evaporate slowly or quickly depending on the substance and other factors. Alternatively, internal releases could be liquid contamination on clothing that has been brought into the building, or some device or container that emits something already in vapour or aerosol, such as a leaking gas cylinder. The most dangerous biological threats are aerosols, either of fine particulates (e.g. the Anthrax used in the USA in 2001) or droplets produced by some sort of spray. Biological liquids, while they may be dangerous on direct contact, do not evaporate into a threatening form. (The carrying liquid, such as water, evaporates but does not bring microbes or biological toxins into the air.)

By looking at these generic categories, there are some very basic assumptions that can be

made. All chemical molecules have a molecular weight. The approximate molecular weight of air is 29 grams per mol. Any gas or vapour with a higher molecular weight than that will be heavier than air. With very few exceptions, the most notable being hydrogen cyanide, chemical and biological threats in gas, vapour, or aerosol form are heavier than air. This does not mean that they won't travel uphill or upstairs, as they can be pushed along by other means such as ventilation. However, it means we can make some basic assumptions about the behaviour of threat materials that will be useful.

A similar precept is that gases, vapours, and aerosols will flow with the air, not against it. Therefore, understanding how and where the air flows in and around a building is a critical bit of knowledge in crafting effective countermeasures. Some premises may have already had airflow studied for the purposes of heating and air conditioning. Specialised consultancies can help in this regard, and there are ways to use computer modelling to assist in understanding how air flows and threat materials behave.

Physical security

Security against C/B threats rests on the bedrock of conventional physical security. Many aspects of security architecture and "Crime Prevention through Environmental Design" provide some degree of benefit in the C/B arena. Many threat scenarios require reconnaissance or the ability to hide a dangerous device. Physical security measures, such as video surveillance, manned guarding, access control, and intrusion detection may serve to deter or prevent hostile reconnaissance or penetration. Control measures such as inspection of packages at entrances can reduce the likelihood of a device being brought into a protected building. Comprehensive coverage by CCTV camera can be a valuable tool in detecting unattended packages and parcels (one possible means of disseminating C/B materials) or can be of value in assessing a possible incident. For example, CCTV operators can notice people being affected by a chemical threat. Additionally, standoff distance from other buildings may achieve some degree of mitigation against external release scenarios, as every meter of distance applies some degree of dilution to an external threat.

Economic principles

As with physical security, few commercial premises can afford a "fortress mentality", either in economic or in practical operational terms. However, there are ways to address the economic impact. Many of the same economic issues that apply to physical security measures apply to C/B countermeasures. Most countermeasures are far easier and less expensive to implement if they are considered early in the design stage. Retrofits to existing buildings are often very expensive. Old and/or historic properties prove difficult to work in under the best of circumstances. Integration of C/B defensive considerations is best done at the earliest part of the design stage for a new building.

Based on the principles cited above, however, some defensive measures will have benefits in realms other than C/B protection. Sometimes it is more economically feasible to advocate for physical security and crime prevention in its own right, with a view that these measures will have protective value in the C/B realm as well. Improvements to ventilation systems may have cause improvements to interior air quality.

Vulnerability analysis

Consider commissioning a professional to conduct a vulnerability survey. A knowledgeable analyst can examine a specific building to point out vulnerabilities particular to the location. Specific vulnerabilities can be mitigated with site-specific countermeasures.

Business Continuity

One of the potential features of C/B terrorism is economic loss due to short or long-term contamination of business premises. The economic losses incurred as a result of a handful of anthrax-bearing envelopes were very large in 2001-20002 in the USA. Property can become unusable for a long period of time, depending on the threat material used, and decontamination efforts will be expensive[1]. Staff members may die or become ill and no longer be able to work. However, sound data recovery and business continuity measures mitigate a large percentage of the theoretical loss. The ability to continue essential business at other unaffected facilities and to devolve responsibilities to other people can partially offset some of the long-term potential losses.

Specific Guidance

The single most useful reference available to date is a United States government document issued by the US Department of Health and Human Services entitled *Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks* (Washington DC, 2002), available as a download[2]. Additional guidance is also available from the Lawrence Berkeley National Laboratory in the US.[3]

Ventilation

Ventilation and air-conditioning systems are ubiquitous in office buildings in modern cities. Much of the breathing air has been handled by a bewildering variety of heating, cooling, ventilation, and handling equipment. Therefore, it is easy to assume that threats that enter the human body through breathing are transported through such systems. Various aspects of building ventilation can be adjusted or retrofitted to improve defence against C/B threats. Building owners and operators are advised to seek professional advice in this regard. It should be noted that the ventilation systems for large buildings are often extremely complex and this subject is worth of hundreds of pages of guidance in itself. Publically available military standards for building and facility protection, also called "collective protection," do exist[4], but are generally prohibitively difficult to implement in normal commercial settings. Some of their principles do make sense, so perusal is still recommended. However, there are some basic concepts which can be more easily implemented that are worth examining.

Filtration

The most obvious ventilation measure is filtration. Hazards can be filtered out of the air. Filtration is more easily done for solids, such as biological aerosols, as they need to be in a specific size range to be absorbed into a human's lungs. A number of types and grades of particulate filtration will provide some degree of protection. HEPA-grade filters provide a high degree of protection against relevant biological threats. Filtration of gases and vapours, which is the primary chemical threat, is much harder. It can be done but requires much larger filters (e.g. activated charcoal) which also have higher air resistance, thus need more hardware to push the air through. Generally, for most likely applications, biological filtration MIGHT be feasible but chemical filtration will not be feasible. It should also be noted that filtration

systems require significant maintenance.

For filtration to be considered a feasible defensive option, overpressure is required. By pushing or pulling more air into the building than it really needs, the air pressure inside the building in higher than the air pressure outside, meaning that air is always flowing out. In practice, this means sealing the whole building, as air will leak out doors, windows, vents, and practically every crack and crevice. A single open window will negate the protective value as overpressure will be lost. Overpressure, if it is combined with filtration, is an excellent defence against external threats. However, overpressure without adequate filtration is worse than doing nothing. With regards to internal threats, overpressure can be a mixed blessing. Overpressure could, in many scenarios, actually work to circulate an internal release to other areas of a building. For this reason, overpressure needs to be executed carefully, with regard to interior air flow, and possibly shut down rapidly in the event of a release of hazardous material inside the building.

Location of intakes

The vast majority of CB threat materials are heavier than air. Many external threats, such as a release of a toxic gas, will travel along with the wind at or very near to ground level. Therefore, building ventilation systems that are close to ground level are in an optimum position for bringing hazardous materials into the building. Ground-level air intakes are also vulnerable to sabotage. Having air intakes on the roof level, or even just one or two floors above street level, provides some degree of defence against CB external hazards. When designing a new building, the design effort should consider intakes at roof level. In many busy cities, this might also serve to reduce intake of traffic pollutants into the building, and could be promoted as an environmental health measure.[5] Basic physical security to restrict public access to air intakes, air handling systems, and return air ducts is not only common sense, but also a basic fundamental improvement to C/B security.

Rapid shutdown

In an emergency situation, it is often helpful to modify the building's ventilation system. This is not always easily accomplished, and many air-handling systems in large buildings are quite complex. Depending on the situation and the system(s) in use, it may be useful to shut down the system completely, reduce or cut off entirely the input of external air, or isolate particular zones of a building.

Handling of incoming parcels, packages, and mail

Parcels and letters can contain dangerous substances. They could contain small dispersal devices or biological powders. The largest instance of fatal biological terrorism in modern times were the anthrax mailings in 2001, described at length in the previous issue of this journal. These instances involved anthrax in the form of a dry powder which easily wafted through the air. As envelopes, parcels, and boxes can contain such potent threats, a high degree of security can be attained by various modifications to procedures for handling arriving material. There are multiple overlapping approaches to this.

One approach is to screen and examine all incoming material. This can also be a useful countermeasure against explosive threats. In order to mitigate threats against the security staff, the incoming material can be opened under fume hoods and/or glove boxes that ventilate their

exhaust safely through filters. This is time consuming and will increase labour expenses. The volume of material to be screened could be reduced by a triage system, whereby expected items from expected senders are not screened as intensively as unexpected items. The screening room where parcels and mail arrives can be segregated from the rest of the building and even have its own air handling system so that any dispersed threats do not affect the rest of the building.

One ancillary approach is to scan paper correspondence so that papers and envelopes do not actually need to go into office buildings in the first place. Few original documents are actually needed in this modern era. A very high percentage of correspondence can be scanned and sent to the recipient electronically.

An escalation of this approach is to physically remove the screening facility to an off-site location. In the post 9/11 operational environment, it is no secret that this is the approach taken by many high risk government buildings. By having all deliveries routed to an alternate location, the threat of dispersal is displaced. Material can be screened at the alternate location and taken by secured means to the office building later. Obviously, this delays incoming material and greatly adds to operational expense. At the highest end, it is possible to subject incoming material to sterilisation by irradiation.[6] It is not a secret that some US government mail is subjected to electron beam sterilisation. This is probably not feasible for most building operators and poses a number of complicated issues beyond the scope of this article.

The effectiveness of screening and remote delivery directly depends on security and employee discipline. If it is easy to circumvent the screening of packages and parcels, then the protective value will be reduced or negated. For some premises, the hassle and inconvenience of strict security procedures may make screening and remote delivery hard to implement.

Incorporate relevant considerations into occupant emergency plans

General office emergency plans usual focus around fire threats or bomb threats. In some locales, they address weather emergencies such hurricanes or tornadoes. However, few occupant emergency plans serious address C/B threat situations. Further complicating the situation is the fact that what may be a sound guideline for an external threat to the building might be the wrong thing to do for an internal release. The normal and understandable reflexive reaction is often “Evacuate the Building” – but this could place many people into a hazardous situation if there is a chemical threat outside the building. Remember, buildings are designed to keep much of the outside environment outside. Most building have some degree of protection from external C/B threats even only by virtue of having doors and windows that can close. But, on the other hand, if the hazard is inside the building, then evacuating people outside, upwind of the building, has great value. Because of these variable factors, occupant emergency plans need to have flexible plans for both internal and external C/B threat scenarios.

Shelter in place

The external threat scenario broadly dictates a “shelter-in-place” response. This means buttoning up inside the building and waiting for the hazard to abate. Much published guidance now exists for shelter-in-place procedures. Generally, a valid shelter-in-place plan includes moving well into the centre of the building, shutting down air-intakes, and closing all windows and doors. Moving upwards in the building is good, as it accounts for the fact that threats are

heavier than air. Provision needs to be made for sufficient space, access to toilets, and water, as a shelter-in-place operation may last for some hours. Due to the multi-tenant, multi-occupant nature of modern office buildings, shelter-in-place planning can get very complicated very quickly.

Detection

There are a wide number of detection and identification sensors widely available, produced largely for military or emergency response purposes. While industry certainly provides some capability in this area, chemical and biological detection and identification is a very complex subject. Detection instruments are sometimes seen as a panacea. But they are not. Sensors are basically information tools. They sense the environment and provide information. Their utility is based firmly on what decisions will be made and what actions will be taken on the basis of that information. The question "what will you do when the detector goes off" more often than not results in an answer of "I don't know". In which case, the money spent on them is best spent on something else.

Various types of chemical detection and identification sensors have some utility in building protection. However, they are quite expensive and need to be used in a rational manner. No chemical detection system is without false alarms, and false alarms and interferents are well-documented in literature[7]. Many are designed around military use cases in field environments and respond to many stimuli in the complex urban environment, such as cleaning chemicals, personal care products and pesticides. If radical responses for false alarms become commonplace, then detection instruments lose their utility as people will ignore them. Biological detection is an area still plagued with inadequacies and the available products are basically either not suitable or too excessively expensive for routine use for commercial buildings. Tread carefully in this area and engage independent advice from experts independent of a sensor vendor.

Use physical security design to mitigate the threat

Visible or easily detected physical surveillance and security measures may serve to modify terrorist behaviour in ways that serve to mitigate the extent of damage causes. As one example, a building operator can place rubbish bins and easily visible CCTV cameras in zones where, due to an air-flow study, the operator knows that air does not readily circulate. If a terrorist device is going to be left in a rubbish bin, then it would function in a location where, due to poor air circulation, it does the least amount of damage. Other measures may be more clandestine in nature. For example, fake air intakes at ground level would easily drive a terrorist dispersal towards that avenue of attack, whereas the real air intakes are at roof level and not visible through reconnaissance from public spaces. These are merely examples, and any such countermeasure would have to be venue-specific.

Inventory and register property

If a building is not accessible for some lengthy period of time due to contamination, a significant amount of goods, equipment and property will be unavailable, possibly indefinitely. Much property may have to be abandoned, destroyed, or subjected to decontamination that damages it. This is one lesson learned from the 2001 US anthrax situation. Having a reasonably current inventory of valuable property, including personal property, can greatly help in making accurate representations to insurers as to actual losses

incurred. Likewise, property that is salvaged and no longer contaminated can be more easily returned to owners. This particular measure also has value in conventional threat scenarios such as fire and explosives incidents.

Dr Gordon Woo Catastrophist, RMS**,** Co-Founder & Editor, Journal of Terrorism and Cyber Insurance

MEDIA INFLUENCE ON TERRORIST ATTACKS

News media coverage is global in geography and continuous in time. Terrorism spans two themes of perpetual international news interest: politics and violence. Terrorism makes news. But the relationship between the media and terrorism is not one way. In fact, there is a deeply symbiotic relationship between terrorism and the media: terrorists depend on the media in crucial ways, and the choice of terrorist attacks is strongly influenced by the consequent media coverage. Gruesome and barbaric attacks that target civilians are sure to attract widespread media coverage. According to Daesh, half of Jihad is media. This has implications for terrorism risk assessment.

The international media responds to all notable events, including terrorism, that help fill the 24-hour news cycle. The relationship between the media and terrorism is not one way. In fact, there is a deeply symbiotic relationship between terrorism and the media: terrorists depend on the media in crucial ways, and the choice of terrorist attacks is strongly influenced by the consequent media coverage. This has implications for terrorism risk assessment.

Risk analysts seek to define a utility function to quantify the reward associated with any risky human endeavour. Utility is a value assigned to an outcome, which may be based on a range of possible metrics. For terrorists engaged in political violence, inflicting wanton harm and economic damage on their adversaries may be rewarded by the satisfaction of revenge and fulfilment of their own sense of justice. A terrorist attack may also be substantially rewarded by the political impact achieved. Rather like television programme ratings, media coverage is a key measure of this political impact. Such coverage serves as free propaganda and recruitment advertising for the terrorist cause.

Political activists may not receive media attention, nor have their ideas publicized, without terrorist action. As the writer Don DeLillo observed, *'Terrorism is the language of being noticed'*. If peaceful protest goes unnoticed, ordinary law-abiding citizens may resort to political violence. Unabomber Ted Kaczynski wanted his thoughts published in The New York Times and The Washington Post. Before this happened in September 1995, he racked up 13 counts of murder and bombing. Hardly anybody would have noticed, let alone read, Anders Breivik's 1,500-page manifesto published online, entitled '2083: A European Declaration of Independence'. Part of the tract details the author's personal reflections prior to his vehicle bombing of government buildings in Oslo, and the mass killing of 69 at an island summer camp on 22 July 2011. Eight died in the vehicle blast, but the tragic loss of so many promising young lives at the summer camp inevitably became the prime focus of Norwegian public grief and international media coverage.

Terrorists like Kaczynski and Breivik can be brought to justice. But even when terrorists are convicted and jailed, they can continue to attract media attention to their political agenda. Over

the course of the years 1980 and 1981, Irish republican prisoners in the Maze Prison outside of Belfast in Northern Ireland launched two hunger strikes for what they regarded as restoration of their status as political prisoners rather than criminals. However, major news outlets such at the *Irish Times* and the *New York Times* refrained from presenting the strikers' demands for political status as legitimate.

The hunger strikes confronted the British government with a public relations crisis. There were disturbing news stories of the hunger strikers withering away, thus allowing the group to gain sympathy and recruitment. The media's role in the hunger strike was important in influencing public opinion. The most celebrated hunger striker was Bobby Sands, who died a martyr to the republican cause on 5 May 1981 after 66 days on hunger strike. Over a hundred thousand attended his funeral, the largest in Belfast, and there was global news coverage of the funeral.

Acutely aware of the strategic consequences of terrorist publicity, it was the British Prime Minister, Margaret Thatcher, who insisted in July 1985 that: *'We must try to find ways to starve the terrorist and the hijacker of the oxygen of publicity on which they depend'*. At that time, publicity outlets were limited to newspapers, print journals, radio and television. Three decades later, a terrorist statement can be disseminated around the world via social media, and a terrorist video uploaded instantly on YouTube. This new technology has transformed the balance of media power between the opposing forces of terrorism and counter-terrorism. Terrorists can now self-publicize their own political agenda. There is some censorship of websites that espouse and incite political violence, but such websites may pop up and close down quite regularly.

In his book on religious terrorism, Mark Juergensmeyer reflected, '*Terrorism without its horrified witnesses would be as pointless as a play without an audience.'* Attraction of a large audience requires publicity. Even comparatively modest terrorist organizations have established professional media departments to manage their publicity. For example, Al Shabab's media department focuses on attracting regional foreign fighters to Somalia from around East Africa, particularly Swahili-speakers, as well as establishing ties with local militant groups. They have featured prominently in the group's propaganda films, including a 2010 recruitment film subtitled in Swahili, Arabic, and English. In West Africa, Boko Haram have created their own audio and video content and distributed it discreetly to journalists on CDs and memory sticks. This is their most potent propaganda tool, with videos including brutal executions and images of the schoolgirls kidnapped in 2014.

Just as with Hollywood action movies, terrorist videos must have dynamic visual action content: shootings, fires and explosions. Most terrorist attacks deliver this kind of visual action, which can be filmed and put to good propaganda effect. By contrast, there are many possible types of terrorist attack modes that are not particularly visual, and would not lend themselves so well to video. Radiological dispersal devices, i.e. dirty bombs, are in this category. The small amount of radioactive material released would lead to low levels of contamination. This would lead to formidable decontamination problems, but the radioactivity would be unlikely to cause any serious health problems or fatalities. Substantial resources would be required to acquire enough quantity of radioactive material, and there is a high interdiction risk associated with its procurement. On 29 June 2007, there was an attempted car bomb attack on the Tiger Tiger nightclub in Haymarket, central London. One of the terrorists was a hospital doctor, with access to radiological equipment. Although the police had dirty bomb concerns, it turned out that the bombers' focus was on causing a massive propane fire and explosion that might have killed large numbers in the night club.

More than contaminating or vandalizing property, killing people generates newspaper headlines, in accord with the classic editorial adage for selling newspapers: if it bleeds, it leads. On 2 November 2011, the Paris office of the satirical magazine, Charlie Hebdo, was petrol-bombed by a Molotov cocktail at 1am, the day after Charlie Hebdo had named the Prophet Mohammed as its editor-in-chief for the week's issue. There was only modest international publicity for this terrorist attack that caused some property damage and publication disruption, but no personal harm to anybody. However, a few years later, on 7 January 2015, the editorial committee of Charlie Hebdo was assassinated in their Paris office by the Kouachi brothers, armed with AK-47s. A million people, including many government leaders from across the world, thronged La Place de la République in Paris the following weekend in solidarity against this terrorist outrage. 'Je Suis Charlie' was tweeted all over the world. Cable news was dominated by these killings, which were perceived as an attack on French liberty itself. A lesson to be learned by terrorist organizations and terrorism risk analysts is that high-profile assassinations leverage the highest media exposure for a given outlay of terrorist resources. This lesson helps explain the terrorist logic of the lone-wolf.

With the massive media attention gained, the benefit-cost ratio for terrorist killings is high. The media outrage against the mass murder of civilians far exceeds the media coverage of infrastructure damage. On 10 October 2015, two bombs were detonated outside Ankara railway station, in Turkey, killing as many as 103 civilians. Counterfactually, the bombs might instead have been detonated on the tracks at night, with few people around. This would have shut down the station, and disrupted the busy railway line to Istanbul. But rail damage can be repaired; lives lost cannot.

Under some circumstances, bombing can be the attack mode of choice if killing civilians is perceived as having too many negative moral repercussions. The IRA had serious qualms about killing civilians because this alienated their key nationalist Irish Catholic constituency. Instead, the IRA provided coded bomb warnings, many of which were disruptive hoaxes, and mastered the development of the fertiliser vehicle bomb to cause massive property loss. Except for such community support circumstances, the media terrorist payoff for murder and executions far exceeds that of large scale criminal vandalism.

Executions can be by shooting, burning, crucifixion, decapitation etc. The more gruesome and barbaric the killings, the bigger and brasher are the headlines. So it was that a UK morning newspaper front page following the brutal killing of fusilier Lee Rigby outside Woolwich barracks on 22 May 2013 had the shocking banner headline 'Beheaded'. The UK media regulator highlighted concerns over a regional news bulletin showing a graphic mobile phone sequence of one of the murderers with a machete and bloodied hands. This was repeated on a loop without audio and without being preceded by a specific warning. Like horror movies, this video nasty was compulsive viewing. Another vile offence against human sensibility that could not be kept off the front pages in February 2016 was the detonation by a 4-year-old small boy of a car bomb containing 4 alleged spies against ISIS. Dressed in a military outfit, he might otherwise have been playing with toy pistols.

In the asymmetric war with nation states, the power of a terrorist group, such as Islamic State, can be projected worldwide by ruthless graphic acts of violence committed against even a modest number of individuals. Disseminated rapidly and amplified globally over the broadcast and social media, such attacks demonstrate a degree of offensive capability that both shocks and terrifies the general population, whilst encouraging its own body of supporters and

aspiring recruits. Terrorist organizations are generally keen to claim credit for successful attacks, including those perpetrated by non-members and others peripheral to the organization, who were just inspired to commit their brutal crimes, but had no direct contact with any members.
The senseless slaughter of pedestrians by truck ramming would be sure to make headline news. On 14 July 2016, a 19 ton refrigerated truck ploughed into the crowd on the Promenade des Anglais in Nice, killing 86. If the truck had been allowed to carry on its rampage for a few hundred metres further, the casualty rate/metre would have been much higher in the most crowded part of the beach zone, close to the site of the Bastille Day fireworks display.

The media had an indirect unwitting role in instigating this bizarre mode of terrorist attack. In December 2015, a car driver apparently under the influence of drink lost control, left the road and hit a restaurant terrace in Nice. This accident was reported in the local Nice Matin newspaper. The driver of the truck on 14 July 2016, Mohamed Lahouaiej-Bouhlel, originally from Tunisia, had kept on his cell phone a photo of this six month old Nice Matin story. What happened by chance can also be copied by those with malicious intent.

A spiral of copycat terrorist attacks can be generated by a whirlwind of media publicity. A few months after the Nice truck ramming, another Tunisian, 24 year-old Anis Amri, killed 12 people and injured 48 others when he rammed a 40-ton truck into a Christmas market in the German capital on 19 December 2016. The truck was fortunately halted by the modern automatic braking system, bringing it to a standstill after about 80 metres. Christmas markets have been targeted by terrorists before: they are open crowded public spaces linked to the religion of the Crusaders. Calls were made afterwards for Christmas markets to be given barrier protection. This would only have deflected an attack to a mass transit or other crowded public space.

Media influence on terrorist targeting

What counts as a successful terrorist operation in a target-rich society has its own geographical political context. In territories, such as Pakistan, where terrorist attack frequency is expressed in events per day, an attack would gain little media attention unless it generated a sufficiently large number of fatalities. In countries of the western alliance, the extent of national surveillance and the diligence of counter-terrorism forces shorten the terrorist attack horizon, and make it difficult for terrorists to execute ambitious plots. Accordingly, in these countries, the attack threshold for gaining media attention is much lower.

Within the western alliance, the utility of a terrorist attack will depend significantly on the media coverage. Crucially, a carefully planned attack with a moderate amount of logistical resources can saturate headline news for days. The Charlie Hebdo committee assassination on 7 January 2015, an attack using simple off-the-shelf military weapons (namely a couple of AK-47s), created an international media storm. Terrorists advertise and promote themselves effectively through their deeds. The maximum expected utility can be achieved by attacks on comparatively soft but high-profile targets. The paramount example is the Charlie Hebdo office in Paris, which was protected only by a single security guard, and had open street access. By contrast, any plot to assassinate a senior political figure would have been much more difficult, because the security would have been tighter.

In 2002, Osama Bin Laden wrote in a letter addressed to Taliban leader Mullah Omar: *'The media war in this century is obviously one of the strongest methods; in fact, its ratio may reach*

90% of the total preparation for the battles'. Three years later, his successor Ayman Al Zawahiri repeated this sentiment, reiterating that Al Qaeda is in a media battle in a race for the hearts and minds of the Umma. This is echoed in the more recent pronouncement of Islamic State that '*half of Jihad is media'*. Terrorists are learning to achieve mastery of the media. In particular, the accomplished multilingual skills of terrorist organizations have made for more effective communication with their diverse international target audience spread across the continents.

In the field of public relations, extensive media publicity about successful terrorist attacks serves as propaganda that can reach the general public automatically and instantaneously, and also manage to influence the policies of democratic governments. The terrorist aspiration might be to persuade or coerce governments to change their policies, through pressure of fearful citizens.

The media can also be used as a means of communicating with governments. An Al Qaeda tape broadcast on Al Jazeera in January 2006 said Al Qaeda was open to a truce with the US if it withdrew from Iraq and Afghanistan. The tape did not say what the conditions for a peace deal were, only that it would be *"a long term truce based on fair conditions ... so both sides can enjoy security and stability under this truce so we can build Iraq and Afghanistan"*. It is not the first time Al Qaeda has offered a truce to the West. Following the killing of 191 people in the March 2004 Madrid railway bombings, a tape recording of Bin Laden offered peace to any European country that stopped *"attacking Muslims or interfering in their affairs"*.

The striving for media attention serves to explain much of terrorist targeting in the western alliance. Terrorist organizations are engaged in an asymmetric war with nation states, which cannot be defeated militarily or economically. The financial cost of terrorism is not measured merely in terms of the loss inflicted by successful attacks, but also by the burgeoning cost of heightened counter-terrorism security. This involves a competitive race between corporations to avoid being the softest target in a class, and hence the lowest hanging fruit to be taken by terrorists following the strategic path of least resistance.

The cost of security may well be more than an order of magnitude larger than the expected economic loss. Public fear and apprehension over terrorism, which are fuelled by alarmist media coverage, drive up the popular demand for ever higher counter-terrorism security expenditure. Ayman Al Zawahiri has cited the escalating cost of homeland security as a circuitous way in which USA can be bled dry economically through terrorism, even if ambitious plots are mostly interdicted.

The intrinsic utility to a terrorist organization of inflicting economic loss through damaging property may not be so significant. But if a terrorist attack fails to gain much media attention, then it would have contributed little to the terrorist cause. Denying terrorists, the oxygen of publicity would be beneficial to counter-terrorism initiatives, if this could be achieved. David Broder of the Washington Post has emphasized that, *'The essential ingredient of any effective anti-terrorist policy must be the denial to the terrorist of access to mass media outlets.'* However, basic democratic rights cannot be infringed, and any step towards restricting editorial authority to headline terrorist attacks would have to be ruled out as unacceptable in a society that values freedom of the press.

The importance of media exposure to the terrorist cause naturally influences their operational decision-making. Given a choice between a speculative vehicle bomb plot on a major urban

building with good street security, and a suicide IED plot against a popular crowded public space in a capital city, the latter would be more reliable and appealing. It would be easier to organize and perpetrate, involve fewer operatives and have a smaller chance of interdiction, and might cause more fatalities which would generate greater media coverage.

Since 9/11, there have been numerous attacks of the latter type: Madrid (2004); London (2005); Boston (2013) and Paris (2015). By contrast, there have been no successful vehicle bomb attacks in countries in the western alliance with substantial terrorism insurance markets: USA, Canada, Australia, UK, France, Germany, Spain, Belgium or Netherlands. In Norway, there has been a successful vehicle bomb attack, perpetrated by Anders Breivik in Oslo. But his day of terrorist mayhem, 22 July 2011, is mainly remembered not for this, but for the mindless and brutal slaughter of dozens of young political activists at a summer camp.

The allocation of resources for counter-terrorism protection should be informed by understanding the importance of the media in terrorist plots. Terrorist targets are more attractive if they have international name recognition, and are well known locally. Terrorist attack modes are more attractive if, like IEDs, they have a distinctive newsworthy kinetic sound and visual impact. Prioritized are locations in which media may already have correspondents and camera crews, and to which media can gain access rapidly. On October 2016, a suspected IED was found on a London subway train. A 19-year-old student was tasered and arrested the following day. If this incident had occurred in a suburban district, it may have gone unreported. The front page headline in the London Evening Standard, '*Armed police on tube to fight terror'*, amplified the impact of this rather minor terrorist incident. Capital cities, and other centres of political, economic and tourist activity, are favoured targets for many reasons, including media coverage.

Dr Shaen Corbet Lecturer, Dublin City University

Shaen has previously worked as an equities trader and with the Financial Stability Department of the Central Bank of Ireland. His research is focused within the fields of financial economics, financial markets, crisis and financial stress measurement, crisis management and the effects of crises upon financial markets.

Constantin Gurdgiev Professor, Middlebury Institute of International Studies, Adjunct Professor of Finance, Trinity Business School

Constantin's research is in investment markets, theory and analysis, and geopolitical and macroeconomic risk analysis relating to financial markets. Professor Gurdgiev serves an adviser to and a board member with AID: Tech, and a co-Founder and Director of the Irish Mortgage Holders Organisation.

FINANCIAL DISRUPTERS: IS THE RISE OF FINANCIAL DISRUPTORS KNOCKING TRADITIONAL BANKS OFF THE TRACK?

The scale and intensity of digital financial criminality has become more apparent and audacious over the past fifteen years. To counteract this escalating threat, financial technology (FinTech) and monetary and financial institutions (MFI) have attempted to upgrade their internal technological infrastructures to mitigate the risk of a catastrophic technological collapse. However, these attempts have been hampered through the financial stresses generated from the recent international banking crises. Significant contagion channels in the aftermath of cybercriminal events have also been recently uncovered, indicating that a single major event may generate sectoral and industry-wide volatility spillovers. As the skillset and variety of tactics used by cybercriminals develops further in an environment of stagnating and underfunded defensive technological structures, the probability of a devastating hacking event increases, along with the necessity for regulatory intervention. This paper explores and discusses the range of threats and consequences emanating from financial digital disruptors through cybercrime and potential avenues that may be utilised to counteract such risk.

The long-term fallout from the 2008 global financial crisis created several deep fractures in traditional-banking models. Most of the sectoral attention today has focused on weak operating profits and balance-sheet performance, especially the risks arising from the negative-rates environment and the collapse in yields in traditional assets, such as highly-rated sovereign and corporate debt. Second-tier concerns in boardrooms and amidst C-level executives[1] relate to the continuously evolving regulatory and supervisory pressures and associated rising costs. Finally, the anaemic dynamics of the global economic recovery are also seen as a key risk to traditional bank's profitability.

However, from the longer-term perspective, the real risks to the universal banks' (and more broadly to the Monetary and Financial Institutions (MFIs)) business models come from an entirely distinct direction. The digital-disruption channels simultaneously put pressure on MFIs' core earnings lines and create ample opportunities for undermining the sector's key unique selling proposition—that is, security of customer funds, data and transactions, and by corollary, enhancing customer loyalty. These channels are:

1. FinTech innovations[2]—including rising data intensity of financial products on offer,
2. Technological threats, such as rising risks to cybersecurity – including both transactional security across counterparties, and customer data., and
3. Second order network threats that arise from cyber security risk exposures relating to rising data intensity of back-office and regulatory compliance operations within the networks of MFIs and their FinTech counterparties.

This three-pronged challenge is not unique to the MFIs, but the scale of its disruptive potential and complexity of the threats compounded by the highly interconnected nature of financial counterparties networks mean that today's traditional MFIs are neither equipped to address nor fully enabled to grasp these threats.

The potential FinTech channels of disruption are further opened by the inability of some financial institutions to update their internal technological structures to meet the demands of clients in both the provision of services and indeed the protection of client's data. In an

environment ripe with economic uncertainty, the financing for these technological upgrades for financial institutions under cash-flow constraints receives little weight due to more immediate areas of necessity for capital provision. This generates an environment where the financial institution must cut costs, yet provide new services, which create added tension and induce new risks into the system, risks that interact with exogenous cybersecurity threats.

Ionescu, Mirea and Blăjan (2011) found that the economic crisis created the incentives and preconditions for a substantial increase in computer crime and fraud, with incidents of illegality presenting exponential growth in the period 2007 to 2011. This growth has also been matched by improvements in the knowledge and technological abilities of computer specialists and internal controllers who are acting to prevent or restrict cyber-crime expansion.

Further evidence of this dilemma has been recently uncovered in the European banking sector, where individual banks and MFIs have been responsible for a multitude of technological mishaps necessitating public apologies. In one such instance, the largest bank in Ireland, Bank of Ireland suffered over ten substantial technological mishaps in the space of twenty-four months between 2014 and 2016 across a range of services include incomplete salary payments, breakdowns in automated payments and indeed the collapse of ATM services. In October 2016, it was announced under the name 'Project Omega' that €500 million would be invested over an expected period over five years to upgrading Bank of Ireland's technological systems to enhance customer services and to introduce operational efficiencies using the Swiss group Temenos to provide software for its new core banking and channels platform (Irish Times, 3 Oct 2016). This investment arrived just after several large scale systems failures in 2012 across the IT systems of the Royal Bank of Scotland (RBS, 2013).

It appears that in many situations, it takes multiple reputational damaging incidents before capital can be located to stem the issue at source. In a deeply competitive environment, this investment solution may not be available to all FinTech companies and, indeed, to all MFIs. Which brings us to the key question that requires examination: do MFIs and their clients and counterparties truly understand the risks that they are taking when using some companies' financial services and products?

Traditional model vs disruptive challenge

Gurdgiev and Saxton (2012) warned that the regulatory and operational nature of banking has been changing through rapid growth in data-rich analytics platforms and tools, as well as through data-enabled product offers coupled with associated growth in demand for data security. Four years since the completion of this work, neither regulatory nor traditional banking models have fully embraced this reality of change. Further, McKinsey & Co. (2015) show how digital disruption is catching traditional banks off-guard, drilling deep into banks' core business lines, selectively targeting higher-margin activities. The study found that 59 percent of established banks' earnings are generated by fee products, including advice, payments, origination, sales and other sub-services relating to lending and deposit offers. These activities yield returns on equity (ROEs) averaging 22 percent, more than 3.5 times the ROE for the balance-sheet provisions and execution components of the loans.

Digital companies (the so-called FinTech sector), large online-services providers (from Apple to Amazon) and service-offer aggregators (e.g., Moneymarket.com) are targeting behaviorally anchored transactions and payments services. This is the cornerstone of the traditional retail banking market, where in 2014, transactions and payments services ranked as the second-

largest source of profits for universal banks. Meanwhile, automated advice systems, along with technology-based lending platforms and capital-raising offers, are taking on the top-ranked profit-generation stream, namely asset management. Coupled with aggregators' products available online, these include pensions and investment products, and insurance. The payments platforms' disruption is already several years into an exponential growth cycle, as are aggregation services. Automated advice and disintermediated lending are just at the early stages of development. Crypto-currencies and blockchain platforms for data transmission, storage and analytics are expanding at an exponential rate. All in, the ability of the technology sector to move fast into established markets along competitive advantage margins based on cost and quality of the offer cannot be discounted. More ominously, the ability of technology platforms to rapidly integrate their offers with other services, such as retail sales and structuring or bundling of consumer services (think of the change from Apple's iTunes to Apple Pay, or from Google and Google+ to Google Wallet), implies that any technological innovation—however disruptive it may be on its own merit—will be ever more challenging for the incumbent players once services bundling can commence.

Unlike traditional banks and broader MFIs, technological platforms in financial services are run on tiny margins, with savings passed to consumers not only via lower costs of services but also via offering broader ranges of services providers and more open platforms for migration across various services provider at lower cost than in traditional MFIs offerings. In other words, unlike traditional MFIs, new services providers, such as NerdWallet, BankBazaar.com, Tencent, LendingHome, Moneysupermarket.com, Airpay, BnkToTheFuture.com, Knab, Sina Weibo and WeChat, and many more, do not rely on capturing consumers in their product-offer nets. Instead, these platforms can offer consumers a range of points at which they can seamlessly enter other platforms and services providers. This model of competitive cooperation is pushing down margins available to those traditional banks and MFIs that engage with new platforms. Preserving market share, retaining clients' lines of business and balancing out the need for deposits with the opportunities for product sales is becoming an ever less and less profitable business for traditional banks and MFIs. In addition, open platform service providers are capturing more efficiently revenues from new sources, currently not available to traditional MFIs, namely data services. Disruptive innovators de facto convert their access to customers into network and data capital that can be monetized by these organizations, but cannot be used to the same extent by the traditional MFIs.

Looking at data from another study from McKinsey & Co., "The Fight for the Customer: McKinsey Global Banking Annual Review 2015", over 2013-2014 the growth in ROE[3] in the global banking industry was driven, to the upside, by the one-offs and indirect returns, such as tax savings, declines in fines and other costs, as well as reduced risk and operating costs. McKinsey found that in the immediate aftermath of the global financial crisis, there was a chorus of bankers reaffirming their commitment to global universal banking because it helped to smooth revenue volatility. A host of regulation, from structural reform to tougher capital and leverage ratios, has changed that. Their analysis shows that genuinely global banks reported average ROEs of around 7.5% in 2013, while large banks with a less diverse business and geographical footprint were able to achieve an average ROE of around 10.7%. Meanwhile, margin increases turned negative, amidst growing external and internal competition pressures. Looking forward into the 2016-2020 horizon, improvements in the underlying interest rate environment, currently touted by many industry players as a panacea to the ongoing margins compression, by incumbent banking-sector executives are unlikely to provide an uplift in margins that could compensate for the corresponding increase in funding costs. Coupled with rising burdens of regulatory-regimes changes, this means that the traditional-banking model

will come under an ever-growing pressure from more agile, less cost-burdened and legacy-weighted technology challengers.

The situation, relating to asymmetric regulatory costs applying to FinTech providers and to traditional financial institutions is set to continue. As noted in Witkowski et al (2016), under the most recent regulatory proposals, U.S. FinTech providers will be eligible for banking licenses bypassing state-by-state permissions. In effect, the federal 'FinTech charter' will be lighter and less burdensome compliance hurdle than the existent full-scale banking licensing processes entail. Added vulnerability of the traditional global banks' business model to technology-enabled challengers comes from the changes in operational and financial trends since the onset of the global financial crisis. Prior to 2008, based on data from Thomson Reuters, the average Tier 1 capital-ratio[4] cushion across the group of globally diversified banks was around 10.5 percent. Since then, the ratio has moved to an average of 12.7 percent in 2012-2014 and is likely to rise further in years to come as banks maintain their adherence to the Basel III Accord[5]. Figure 1 presents evidence of the changing Tier 1 capital-ratios in a diversified selection United States, European and worldwide banks between 2006 and 2015. Beyond quantitative aspects of the Tier 1 ratio, improving the quality of underlying capital assets will further increase the overall costs associated with capital cushions. This will add to other significant margin pressures faced by banks.

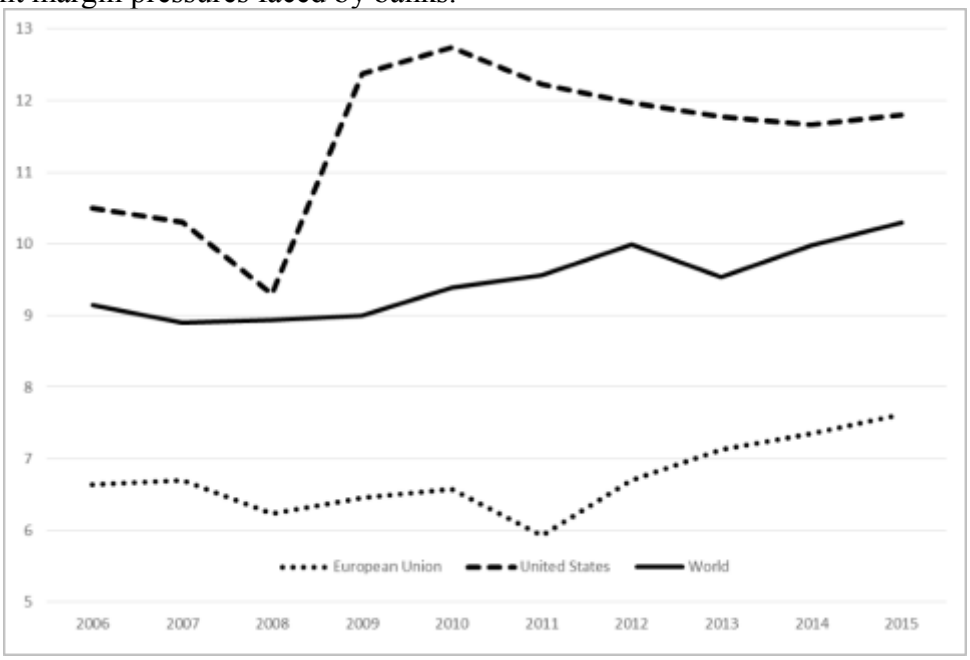

Figure 1: *Capital Tier-1 ratios in the largest United States, European and Worldwide banking institutions (2006-2015). Source: The World Bank.*

Meanwhile, deleveraging during the global financial crisis has meant that loans-to-deposits ratios in advanced economies fell from approximately 129 percent during the crisis to 108 percent today. Figure 2 presents evidence of the European loan-to-deposit ratio which peaked at over 140 percent during the height the financial crisis. The resulting decline in loans-assets profitability was partially offset by increases in leverage ratios in emerging markets, where the loans-to-deposits ratio rose from 76 percent prior to the onset of the financial crisis to more than 80 percent today. The trouble is that emerging markets have just entered the period of structural deleveraging. Added trouble develops when considering that this geographic segment of the financial-services market is now the main arena for competition between traditional MFIs and the FinTech-enabled challengers. In other words, traditional MFIs are not

only about to experience a dual squeeze on their profitability from the structural changes ongoing in the emerging markets, but they are also ever more vulnerable to such risks in the current environment of secular stagnation in advanced economies and deleveraging processes in the emerging markets.

Figure 2: *Average European loan-to-deposit rates (1998-2016). Source: European Central Bank.*

Thus, in a way, an apt analogy between today's traditional MFIs and their FinTech disruptors is that of the early 20th century competition between the established, highly capitalized and legacy-weighted railroads and the strategically agile, more innovative carmakers with far less risky capital structures and leaner operating systems. Starting from the dominant position, the former witnessed their complete loss of high-value-added customers (passengers and time-sensitive, high-value cargo) to the latter within a span of a few decades. Adjusting for the speeds at which modern technology emerges and is deployed, the same process will take years, not decades, to complete in the banking sector of the 21st century.

The darker side of technology

If, in the above analogy, FinTech acts as the car industry to traditional banking's "railroad-like" business model, then the other side of the technological revolution is pushing armies of train robbers onto the train tracks. While competitive pressures are rising fast, the disruptive nature of data-enabled technological innovations is also being felt on the side of systems stability and in the realm of cybersecurity. Rollins and Wilson (2007) found that the US and international community have taken some steps to coordinate laws to prevent cybercrime, but if trends continue, computer attacks would become more numerous, faster and more sophisticated. The Government Accountability Office stated that US government agencies may not in the future be able to respond effectively to such attacks.

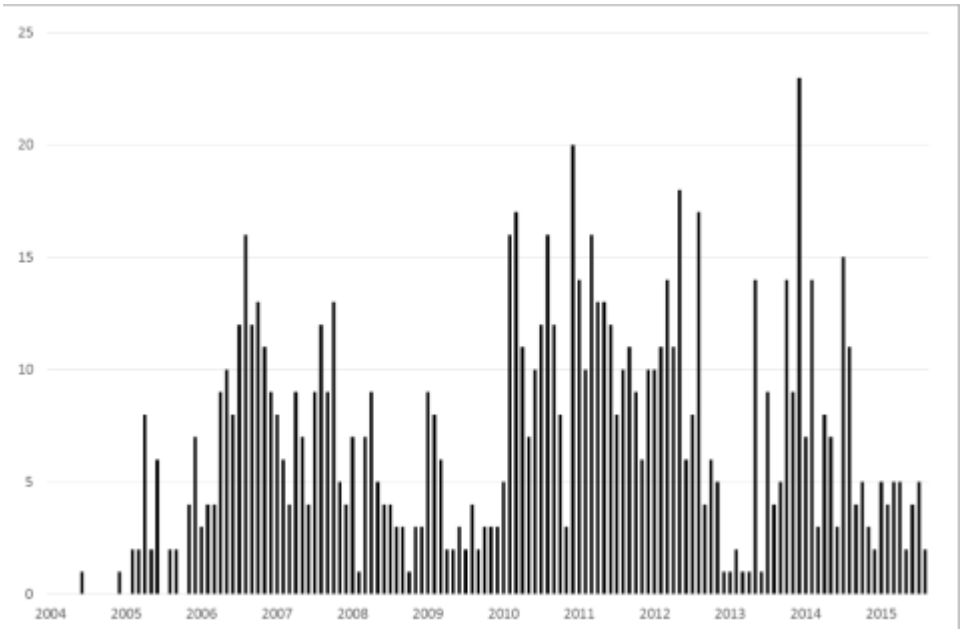

Figure 3: *The frequency of cybercrime events targeting publicly traded companies (monthly, 2004-2015). Note: The full sample period extends from January 2004 to August 2015. Only events where company statements and mainstream media reports have been issued are included. Source: Corbet and Gurdgiev (2017).*

Haines and Johnstone (1997) identify the numerous methods through which cybercrime can occur, finding that advances in communications, information systems and cyber electronic innovations increasingly dispel the myth that crime stops at the border, where Anderson et al. (2013) found that the indirect costs and defence costs of cybercrime are much higher for transitional and new crimes. Overvest and Straathof (2015) report the findings of the econometric study into the linkages between the depth of the internet coverage and the extent of the cybercrime. They state that their "results suggest that a ten percent increase in the number of internet users worldwide raises the number of attacks by about eight percent. Bandwidth in the country of origin and economic ties are also significantly related to attacks.

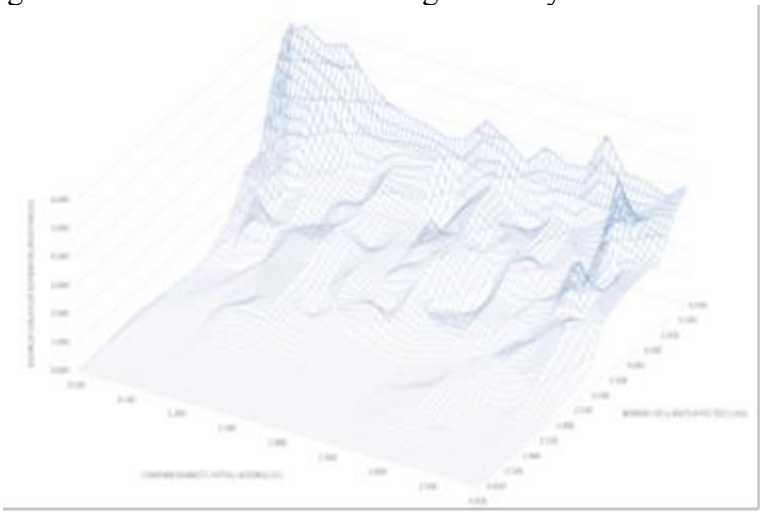

Figure 4: *Volatility spillovers due to data breaches compared to the company market capitalisation and number of clients records affected. Note: Records lost represents the log of the recorded estimated size of the data breach as measured by the number of customers affected. Source: Corbet and Gurdgiev (2017).*

Corbet and Gurdgiev (2017) found that corporations with large data breaches are punished

substantially in the form of stock market volatility and significantly reduced abnormal stock returns after experiencing the impact of cybercrime or a hacking event. The authors use data from public sources to identify, classify and analyse all major events relating to cyber-hacking and cybersecurity crises in the world of publicly traded companies, including major banks and MFIs. In the banking sector alone, for example, 2012 saw 79 attacks involving exposure of client information, while in 2013, some 20 financial companies were targeted by concerted distributed denial-of-service attacks (DDoS). Figure 3 presents evidence in the increasing frequency of hacking events since 2004. Companies with lower level of market capitalisation are found to be most susceptible as presented in Figure 4. In an environment where corporate data protection should be paramount, minor breaches appear to be relatively unpunished by the stock market, but there is significant evidence presented of a growing importance in the contagion channel from cyber security breaches to stock market volatility.

These risk-transmission pathways are reaching beyond the known channels for spillovers between the share prices of the company subjected to cybercrime. Instead, they are impacting trading and portfolio links, institutional structures such as international subsidiaries, and constitute systemic-contagion effects. Using an EGARCH methodology, we investigated the stock market volatility spillovers across publicly traded equities generated in the immediate aftermath of a hacking event over a period from 2000 to 2015. Our samples of such events include more than 850 occurrences of data losses and prioritize these events in terms of the size of the target company, the type of cybercrime and the number of client records affected. Of the different types of cybercrime included, hacks are by far the most frequent type of attacks and appear to be targeted at higher-value companies. This may indicate that some of these companies may have superior security systems in place to mitigate physical theft of data devices and insider-triggered releases of data. In contrast to physical security measures, the increased sophistication of hacking appears to be more than capable of targeting large companies and banks and MFIs. The frequency of success and the size of attacks also appear to be correlated in time. Of the 29 reported large hacks that occurred between 2005 and 2011, 21 events have generated volatility contagion across the markets. In comparison, over the 2012-2015 period, there were 34 identifiable data-breach or hacking events in our dataset, implying a rapid rise in the number of such events compared to the 2005-2011 period. More worryingly, of 34 events, 25 attacks resulted in contagion.

CPMI-IOSCO (2016) warn about the potential for cyber security risk to monetary and financial institutions (MFIs) becoming systemic through contagion effects, and call for pre-emptive testing of MFI systems as “an integral component of any cyber resilience framework”, stating that “all elements of a cyber resilience framework should be rigorously tested to determine their overall effectiveness before being deployed within an FMI, and regularly thereafter.” Similarly, Dahlgren (2016) warn that “cyber threats pose a potentially systemic risk to financial stability through the disruption or corruption of critical payment, clearing and settlement systems and related data.” A glaring and obvious omission on this list is a failure to include other potential channels for systemic risk transmissions, including exchanges and over-the-counter markets. Beyond the systemic nature of the threat, the magnitude of costs and disruptions imposed onto the economies by cyber-attacks is growing.

Over the course of 2014, some 35 percent of the data thefts were from website breaches, 22 percent were from cyberespionage, 14 percent occurred at the points of retail sale, and 9 percent came from the use of credit or debit cards. Which implies that the risk of cybercriminals exploiting core banking-services channels for potential vulnerability was roughly four times more likely than retail-services channels. The presence of big data-based FinTech-services

providers and other non-banks offering ebanking-related products complicates the picture, as recently noted by Packin and Aretz (2016). However, to date, data from disclosed hacking and other cyber attacks on publicly listed companies does not support an assertion that FinTech challengers are themselves more prone to cybersecurity failures. Instead, traditional banks and MFIs appear to be more the sitting ducks for cybercriminals. As noted by Robert Anderson, executive assistant director of the FBI's Criminal, Cyber, Response, and Services Branch: "*We're in a day when a person can commit about 15,000 bank robberies sitting in their basement*."

The Ponemon Institute's study published in 2015 found that the total cost of data breaches across corporate sectors rose 23 percent year-on-year in 2014, with cyber attacks now accounting for 47 percent of all data-breach cases in 2015, up from 37 percent in 2013. In one recent attack, carried out by Russian hackers, the account data of some 76 million financial-services clients was stolen from a global banking institution. And, as claimed by the FBI, nearly 519 million financial records have been stolen from US companies by hackers within the period of 12 months prior to October 2014. And Russian hackers allegedly acquired more than 150,000 press releases from Wall Street publications in August 2015. It is claimed that this data was then used to gain a trade advantage, worth $100 million (Riley, Robertson and Geiger, 2015). In another attack this year, the entire business community of the Cayman Islands was targeted by concerted efforts to breach IT (information technology) systems security. As revealed in an indictment, unsealed in 2016, in 2011 a group of Iranian-sponsored hackers launched attacks against 46 Wall Street institutions, including the New York Stock Exchange and NASDAQ (Larson, Hurtado and Strohm, 2016).

McAfee (2013) reported that the estimated financial gains from cybersecurity breaches to be in the realm of $120 billion in the US alone, with "the cost of identity theft using cyber techniques in the US" at $780 million. Other sources of cybersecurity-related losses by US banks, excluding other MFIs and intermediaries, were estimated at between $300 and $500 million a year. Projecting these loss estimates into 2016, based on historical growth rates in cyber attack frequencies and severity, banking-sector losses in the US alone arising from cybersecurity breaches could reach USD 1.9 to 2.46 billion. According to the EU authorities, as reported by Stearns (2016), "network security incidents resulting from human error, technical failures or cyber attacks cause annual losses of 260 billion euros ($288 billion) to 340 billion euros." And despite the common perception that cyber security vulnerabilities apply primarily to private sector companies, evidence is mounting that central banks and regulators themselves are not immune to cyber-crime. In spring 2016, the Bangladeshi Central Bank became a victim of a cyber-attack resulting in a theft of $81 million (Finkle and Spicer, 2016). Whereas, in May 2016, the Greek Central Bank became a victim of a hack by the Anonymous group (Georgiopoulos, 2016).

Despite the executives' rhetoric about the urgency of preparing traditional banks and MFIs for cybersecurity challenges, banking institutions continue to treat cybersecurity as a non-strategic matter. Three major cybersecurity exercises carried out in recent years in the US, UK and Canada, such as SFIMA-organized Quantum Dawn, CBEST and IIROC (Investment Industry Regulatory Organization of Canada) scenarios testing, all exposed significant areas of concern when it comes to the financial sector's ability to counter systemic risks associated with cybercrime. More ominously, the results also indicate that at the organizational level, major banks and MFIs continue to treat cybersecurity as a technical challenge, to be handled by the IT departments and monitored by compliance and siloed audit functions, rather than a strategic threat to be prioritized across the entire organizational structure through fully integrated

enterprise risk management systems, from the board to the lower tiers of management.

It is worth noting that the utilised hacking-events database is predominantly reflective of the private-sector episodes. At the same time, as several high-profile events cited above suggest, financial-services providers are also witnessing increasing risks of state-sponsored cybersecurity attacks. In fact, Lin (2016) deals with the latter issue of "new tensions relating to financial hostilities, cyber attacks, and non-state actors posed by financial warfare". In a recent high profile episode, SWIFT, or the Society for Worldwide Interbank Financial Telecommunication, a global messaging platform used by some 11,000 financial institutions worldwide, was exposed to a series of threats of cyber incidents. In these, "malicious insiders or external attackers have managed to submit SWIFT messages from financial institutions' back-offices, PCs or workstations connected to their local interface to the SWIFT network" (Finkle, 2016). Although the systems of the SWIFT platform itself were not compromised in these incidents, malicious messages were, it appears, submitted to the SWIFT networked clients. In an unrelated case, $81 million was stolen in February 2016 from Bangladesh's central bank. SWIFT CEO Gottfried Leibbrandt stated that "*hackers successfully breached the systems of two banks over the summer and a third bank had repelled an attack*". SWIFT was forced to issue a security update on 20 September 2016 and deploy a "*new customer security programme – a dedicated initiative to reinforce and evolve the security of global banking*" (SWIFT, 2016).

Corbet and Gurdgiev (2017) propose two potential regulatory alternatives where hacktivists may actually provide regulatory and enforcement benefits. This may initially appear a-theoretical, but is anchored to the already evolving markets for hacktivist services in detecting and preventing potential weaknesses in corporate cybersecurity infrastructure[6].

The first view is that hackers and hacktivists, if appropriately remunerated and monitored, could provide the necessary skillset to act in a regulatory capacity and offer benefits to corporate technological infrastructures in the form of identifying structural cyber-security weaknesses[7]. Public disclosure in this scenario may in fact be more beneficial as a punishment alongside regulatory fines.

This leads to a second view, where regulatory authorities can maintain their current technological capabilities as hackers' skillsets and tools develop. To the extent that regulators may themselves lack the necessary skillset to monitor hacking activity, direct engagement with hacktivists can provide invaluable access to the skills and tools that regulatory authorities often lack. In traditional responses to hacking threats, hackers first breach company or organisation data systems and cause unprecedented reputational damage to the companies, therefore imposing severe costs on consumers. Subsequent to this, regulatory authorities spend time and resources identifying who has caused the breach, mitigating the breach costs and pursuing prosecution of those responsible.

Quite simply, in current environment, regulators chase hackers after the damage is done, while companies remedy the cost of breaches through insurance and by ex-post systems upgrades. In our proposed preventative channel, hacktivists and regulatory authorities can work together under a model of effective monitoring and remuneration, instead of opposing each other. In an environment where the size and intricacy of data breaches are becoming more advanced and sophisticated, more pressure must be placed on corporate mechanisms to protect consumer's data across all sectors.[8]

Coupled risks

The twin developments of FinTech-led creative disruption and the hacking-led cybersecurity threats are hitting at the heart of the already weakened traditional-banking model. The very core of this model relies on customer "stickiness" or loyalty in order to upset existent basic-services clients into higher-margin products. But the loyalty of these customers is currently on a decline, in part due to the technology challenges and in part due to traditional banks and MFIs' strategic failures to prioritize customer service and engagement.

In its 2015 study of the core-banking sector's operations and strategy, IBM's Institute for Business Value found that the gap between banking executives' perceptions of the quality of their customer service and their clients' views of the same is as wide as ever. In retail banking, IBM found that 62 percent of industry C-level leaders think they deliver excellent customer service. Only 35 percent of the industry's customers agree with such an assessment. The gap was even wider in the case of higher value-added lines of business, such as asset management, where 57 percent of wealth-management executives believe they provide an excellent experience, while only 16 percent of their customers agree. Matters are even worse in the key areas of creating a personalized customer experience, encouraging customer loyalty and building customer trust. The latter issue is paramount to a bank's ability to retain key lines of business from their clients. As many as 96 percent of bankers believe their customers trust them more than other non-bank competitors. Only 67 percent of customers actually trust their primary bank compared to other bank competitors. Controlling for wide-spread faming and anchoring biases in financial services, the percentage of the banking customers with organic trust in their providers is probably lower than that.

The window for technological disruption in the traditional or universal banking model, opened by technological developments of 2004-2007 and widened by the global financial crisis of 2008-2011, has now been blown off its hinges by the sheer size of the incoming disruptors from the likes of Google and Apple. And the winds of technological and data changes are getting ever stronger.

Concluding comments

This paper has explored and discussed the threat and consequences emanating from financial digital disruptors through a host of channels including direct cybercrime. The global recession has created several deep fractures in the traditional banking model. Attention appears to be now focused on purely financial risks in the FinTech and banking markets such as capital Tier-1 buffers and solvency, which has created an opportunity for financial hackers to exploit. Current evidence suggests that the scale and intensity of these financial crimes are becoming more and more apparent and audacious.

Potential FinTech and banking channels of disruption have been further exacerbated by significantly reduced funding which is necessary to upgrade internal technological infrastructures to protect against cyber criminality. As these digital disruptors evolve in skill and technological capacity, the security systems necessary to defend against this risk appear to be stagnating due to cost-savings driven by sectoral competitiveness and regulatory restrictions in the form of capital buffers. In effect, as regulators have attempted to reduce the risk of financial crises, they may have inadvertedly increased risks stemming from fraudulent and criminal behaviour. It could only be a matter of time before these technological defences are completely overwhelmed. Further, this generates a dislocation in the risks that FinTech and

banking customers are truly being exposed to, when in fact these technological risks are as substantial as liquidity or banking crises in the companies whose services they may utilise on a daily basis. Moreover, Corbet and Gurdgiev (2017) have found significant contagion channels after recent hacking events, which indicates that a single hack may generate sectoral and industry-wide volatility spillovers.

The selected response by FinTech companies, MFIs and regulators alike to technological security breaches appear to be post-event at present rather than preventative. These responses are also excessively reliant on securing general cybersecurity insurance coverage, further reducing internal incentives for MFIs to undertake active ex ante measures to prevent cyber risks. As the skillset and range of tactics used by cybercriminals develop in an environment of stagnating and underfunded defensive structures, the probability of a devastating hacking event further increases. The damage and loss generated by digital disruptors can no longer be seen simply as a cost of doing business.

References

Bloomberg (2016), "Iranians Hacked From Wall Street to New York Dam, U.S. Says", March 24, 2016. http://www.bloomberg.com/news/articles/2016-03-24/u-s-charges-iranian-hackers-in-wall-street-cyberattacks-im6b43tt

Corbet, S. and Gurdgiev, C. (2017), "Regulatory Cybercrime: Can Hacking Provide a Mechanism to Regulate Corporate Technological Structures" working paper, forthcoming.

CPMI-IOSCO (2016). "Guidance on cyber resilience for financial market infrastructures", June 2016, Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions Guidance on cyber resilience for financial market infrastructures, ISBN 978-92-9197-288-3

Dahlgren, S. (2016) "The Importance of Addressing Cybersecurity Risks in the Financial Sector" March 24, 2015 Remarks at the OpRisk North America Annual Conference, New York City

Dietz, M., Härle, P. and Khanna, S. (2016), "A digital crack in banking's business model", McKinsey & Co., April 2016. http://www.mckinsey.com/industries/financial-services/our-insights/A-digital-crack-in-bankings-business-model?cid=digistrat-eml-alt-mkq-mck-oth-1604

Finkle, J. and Spicer, J. 2016. "U.S. warns banks on cyber threat after Bangladesh heist" Reuters, Tue Jun 7, 2016. http://www.reuters.com/article/us-cyber-heist-regulator-idUSKCN0YT25H

Georgiopoulos, G, 2016. Anonymous attack Greek central bank warns others, Reuters, May 4. http://www.reuters.com/article/us-greece-cenbank-cyber-idUSKCN0XV0RR

Global Risk Insights, 2016. "Is Wall Street cyber secure?" April 21. http://globalriskinsights.com/2016/04/wall-street- cyber-security/

Gurdgiev, C. and Saxton, K. (2012), "Data: a core challenge for financial regulatory reform", Central Banking, February 2012. http://www.centralbanking.com/central-banking-

journal/feature/2153889/-core-challenge-financial-regulatory-reform

Haines, J., Johnstone, P., 1997. Global cybercrime: New toys for the money launderers, Journal of Money Laundering Control, 2(4), pp. 317-325.

Hancock, C., 2016. Bank of Ireland to spend €500m on enhancing software, The Irish Times, 4 October, http://www.irishtimes.com/business/financial-services/bank-of-ireland-to-spend-500m-on-enhancing-software-1.2815284

IBM (2015), "Banking redefined disruption, transformation and the next-generation bank", IBM Institute for Business Value. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=XB&infotype=PM&htmlfid=GBE03704USEN&attachment=GBE03704USEN.PDF

Ionescu, L., Mirea, V., Blăjan, A., 2011. Fraud, corruption and cybercrime in a global digital network, Economics, Management and Financial Markets, 6(2), pp. 373-380.

Kelly, E., "Officials warn 500 million financial records hacked", USA TODAY, October 20, 2014. http://www.usatoday.com/story/news/politics/2014/10/20/secret-service-fbi-hack-cybersecuurity/17615029/

Kelly, Meghan (2013) "From dark days to white knights: 5 bad hackers gone good" Venture Beat, November 8, 2013; http://venturebeat.com/2013/11/08/black-to-white-hat/.

Larson, E., Hurtado, P., Strohm, C., 2016. Iranians hacked from Wall Street to New York dam, US says, Bloomberg, 24 March, https://www.bloomberg.com/news/articles/2016-03-24/u-s-charges-iranian-hackers-in-wall-street-cyberattacks-im6b43tt

Lin, T. C. W., "Financial Weapons of War" (April 14, 2016). Minnesota Law Review, Vol. 100, p. 1377, 2016. Available at SSRN: http://ssrn.com/abstract=2765010

McAfee (2013), "The Economic Impact of Cybercrime and Cyber Espionage", Center for Strategic and International Studies, July 2013. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf

McKendry, Ian and Macheel, Tanaya (2015) "Regulators to Step Up Cybersecurity Activity: Lawsky", American Banker, July 28, 2015, http://www.americanbanker.com/news/bank-technology/regulators-to-step-up-cybersecurity-activity-lawsky-1075715-1.html.

McKinsey & Co. (2015), "The Fight for the Customer: McKinsey Global Banking Annual Review 2015", September 2015. http://www.mckinsey.com/industries/financial-services/our-insights/the-fight-for-the-customer-mckinsey-global-banking-annual-review-2015

Overvest, B. and Straathof, B. (2015) "What drives cybercrime? Empirical evidence from DDoS attacks" April 24, 2015, CPB Netherlands Bureau for Economic Policy Analysis, CPB Discussion Paper 306.

Packin, N. G. and Aretz, Y. L., "Big Data and Social Netbanks: Are You Ready to Replace Your Bank?", February 19, 2015. Houston Law Review, Vol. 53, No. 5, 2016, Forthcoming. Columbia Public Law Research Paper No. 14-460. Available at

SSRN: http://ssrn.com/abstract=2567135

Ponemon Institute, "2015 Cost of Data Breach Study: Global", May 2015. http://ibm.co/1FStqBu

Finkle, J., 2016. SWIFT discloses more cyber thefts, pressures banks on security, 31 August, http://www.reuters.com/article/us-cyber-heist-swift-idUSKCN11600C

RBS Group. 2013. RBS Group Summary in relation to the major IT systems failure affecting the RBS Group in June/July 2012, response and remediation plans March 2013. http://www.rbs.com/content/dam/rbs/Documents/News/2014/11/RBS_IT_Systems_Failure_Final.pdf

Riley, M., Robertson, J., Geiger, K., 2015. Russian Hackers of Dow Jones said to have sought trading tips, Bloomberg, 17 October, https://www.bloomberg.com/news/articles/2015-10-16/russian-hackers-of-dow-jones-said-to-have-sought-trading-tips

Rollins, J., Wilson, C., 2007. Terrorist capabilities for cyber attack: Overview and policy issues, Focus on Terrorism, Nova Science Publishers, New York, Volume 9, ISBN: 978-1-60021-709-8, pp. 43-63.

Stearns, J., 2016. European Union's First Cybersecurity Law Gets Green Light, July 6, 2016, Bloomberg. https://www.bloomberg.com/news/articles/2016-07-06/european-union-s-first-cybersecurity-law-gets-green-light

SWIFT, 2016. SWIFT announces new security tool to strengthen customer fraud controls, Press Release, Brussels, 20 September, https://www.swift.com/insights/press-releases/swift-announces-new-security-tool-to-strengthen-customer-fraud-controls

Witkowski, Rachel, Demos, Telis and Rudereair, Peter (2016) "Regulator Will Start Issuing Bank Charters for FinTech Firms", Wall Street Journal, December 2, 2016, http://www.wsj.com/articles/regulator-will-start-issuing-bank-charters-for-fintech-firms-1480691712

Whittaker, J., "Hackers hitting Cayman companies: Ransomware scams a key concern for business", April 12, 2016. https://www.caymancompass.com/2016/04/12/hackers-hitting-cayman-companies/