Institution: University of Cambridge

Unit of Assessment: UoA17 Business and Management Studies

Title of case study: Developing cyber risk management for Lloyd's of London and the wider (Re)insurance sector

Period when the underpinning research was undertaken: 2015 to date

Details of staff conducting the underpinning research from the submitting unit:

Name(s):	Role(s) (e.g. job title):	Period(s) employed by submitting HEI:
Daniel Ralph	Professor, Director, Centre for Risk Studies	Mar 2000-present
Edward Oughton	Postdoctoral Researcher, Senior Postdoctoral Researcher	Jun 2015– Apr 2018
Simon Ruffle	Director of Research and Innovation	Apr 2014-present

Period when the claimed impact occurred: January 2016 to date

Is this case study continued from a case study submitted in 2014? N

1. Summary of the impact (indicative maximum 100 words)

Cambridge Centre for Risk Studies (CCRS) has established itself at the forefront of research into cyber risk insurance products and cyber risk management internationally. The research has provided a disciplined approach to building threat taxonomies and populating cyber risk categories with scenarios and models to recognise and then quantify commercial exposure to cyber threats. This has been used by a number of organizations across the sector, namely: a risk modelling company, Risk Management Solutions (RMS), to build and sell cyber catastrophe risk models to the cyber insurance industry; an insurance company, Pool Re, to underpin its new, since 2018, cover of cyber terror insurance; and an insurance regulator and market facilitator Lloyd's of London to manage the financial risk reporting of its syndicate members regarding cyber insurance products.

2. Underpinning research (indicative maximum 500 words)

Cambridge Centre for Risk Studies (CCRS) at the University of Cambridge was founded in 2009 to study systemic risk; specifically, to bring research into systemic risk into focus in corporations across all sectors and to provide business-ready frameworks and tools to manage systemic risks. The need for the research was not obvious at the time to professional risk managers who traditionally ignored threats outside their control. But it was obvious to the main constituents of the CCRS business community; senior officers in global corporations as well as government departments and long-term investors, following the global financial crisis in 2008, a prototypical systemic event.

Research undertaken specifically on cyber risk by CCRS in the period has focused on quantifying the scale of the threat in the form of losses to the economy (gross domestic product) or in the context of insurance companies, cyber insurance payouts. Several research foci run through the work: (i) structuring identification of threats which can cause loss or damage, which has led to the development of risk taxonomies and their corresponding evidence base [**R2, R3, R4**]; (ii) using the evidence base for each threat type to model loss processes that connect causes to effects (damage or loss), and thereby codify what is systemic about risk [**R1, R3, R5**]; and (iii) making impact assessments concrete and auditable by constructing counterfactual scenarios for use as stress tests, either quantified narratives [**R3, R5**] or numerical models [**R1**].

Initially CCRS identified a variety of cyber information technology (IT) threats such as data exposure or theft, or extortion in which an IT system is made inaccessible until a ransom is paid. In [**R3**] research categorises and then models, as counterfactual scenarios, the top five cyber IT threats to provide cyber insurance stress tests. In order to translate these stress tests into cyber insurance payouts, the report [**R2**] provides a data schema to model the insurance loss process, to break down the policies of insurers and attribute different payouts to different policies depending on the scenario under consideration. These reports constitute a model design of how to quantify the total policy payouts that an insurer might face at a single point in time, due to an extreme but plausible cyber event, something so severe that it might happen only once in a century. This analysis is a key determinant of the level of cash reserves ('regulatory capital') that an insurer must hold in order to satisfy the regulator that it will be able to honour its promises to policy holders. The research was recognized for its originality as there were no cyber risk model precedents and almost no insurance loss data to work with at the time the research was conducted.

In addition to cyber IT threats, research has also highlighted that cyber operational technology (OT) threats carry the risk of both physical damage (e.g., [**R5**]) and operational disruption (e.g., [**R1**]) by disabling or commandeering a control system for an industrial plant or physical infrastructure such as a power generator. This identified an important new level of understanding for risk managers, including those in the insurance industry, who had previously assumed that physical consequences naturally have a physical root cause.

In widely reported 2015 work [**R5**], researchers provided important analysis which demonstrated that physical damage to power generators could be engineered at a mass scale, causing blackouts to millions of people along the East Coast of the USA over a prolonged period. This has had substantial and ongoing impact for risk regulation of insurance companies described in section 4 (Lloyd's). This was consolidated in a 2016 data schema for calculating insurance exposure [**R2**], covering IT and OT losses. Further work [**R4**] showed the potential for cyber terrorists to inflict physical damage to industrial plants and commercial real estate. The scale of disruption loss was explored in the context of a cyber attack on UK electricity distribution networks in the 2019 publication [**R1**], which quantified how power outages cascade to nationwide disruption of transportation, water and other infrastructure services.

3. References to the research (indicative maximum of six references)

R1. EJ Oughton, D Ralph, R Pant, E Leverett, J Copic, S Thacker, R Dada, S Ruffle, M Tuveson, JW Hall (2019). Stochastic Counterfactual Risk Analysis for the Vulnerability Assessment of Cyber-Physical Attacks on Electricity Distribution Infrastructure Networks. *Risk Management: an International Journal*, Vol. 39, No. 9, 2012-2031. DOI: 10.1111/risa.13291.

R2. Cyber Insurance Exposure Data Schema v1.0 (2016). Centre for Risk Studies, University of Cambridge Judge Business School. Centre for Risk Studies authors: A Coburn, S Ruffle, E Leverett, A Skelton, J Copic, A Rais-Shaghagi.

R3. Managing Cyber Insurance Accumulation Risk (2016). Centre for Risk Studies, University of Cambridge Judge Business School in collaboration with Risk Management Solutions, Inc. Centre for Risk Studies authors: A Coburn, S Ruffle, E Leverett, A Skelton, J Copic, S Sweeney, A Rais-Shaghagi, V Kesaite, S Kelly, D Ralph, M Tuveson, L Pryor, T Evan.

R4. Evan, T.; Leverett, E.; Ruffle, S. J.; Coburn, A. W.; Bourdeau, J.; Gunaratna, R.; Ralph, D. (2017). Cyber Terrorism: Assessment of the Threat to Insurance; Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge.

R5. Business Blackout: The insurance implications of a cyber attack on the US power grid. Centre for Risk Studies, University of Cambridge Judge Business School, Lloyd's Emerging Risk Report – 2015 Innovation Series (2015). Centre for Risk Studies authors: S Ruffle, E Leverett, A Coburn, J Copic, S Kelly, T Evan.

Quality of research: R1 is a peer reviewed journal publication. For R2-5, CCRS was nominated for two industry awards: Risk Modeller of the Year, *Reactions* 2018 and Advisen Cyber Risk Innovation of the Year 2018. R2 is being considered as a standard by the insurance industry Association for Cooperative Operations Research and Development, ACORD. R5 has been subject to particular scrutiny given its adoption by Lloyd's of London for risk reporting by its syndicate members.

4. Details of the impact (indicative maximum 750 words)

Cambridge's Centre for Risk Studies (CCRS) has established expertise in developing scenarios and applying and disseminating research into systemic and emerging risks. CCRS has been influential in helping companies in various sectors, notably insurance, to manage new or newly recognised risks. It has done so by engaging directly with organisations to produce research outputs which are immediately applicable to those sectors engaged in assessing and managing cyber risks. Throughout its ten-year history the centre has prioritised the rigour of its research as the basis for engaging with industry and policy makers internationally and nationally through a variety of formats (interviews, invitational and public events, sponsored research projects, research papers, and blogs) in order to continually ensure that its agenda and outputs have meaning in the business community. Many research projects are collaborations with corporate partners. The centre's annual Risk Summits [**S5**] are aimed at challenging and being challenged by corporate managers, with strong academic and practitioner inputs, rather than simply dissemination events for research. Cyber risk featured in CCRS's first annual meeting with respect to control of electricity and telecommunications. It has been a key threat type since the creation of the centre's first risk taxonomy [**S6**]. Impact is presented in three main areas; cyber insurance risk modelling with RMS, cyber terrorism risk assessment with Pool Re, and cyber risk scenarios for insurance companies with Lloyd's of London.

An important CCRS contribution to managing risks to cyber insurance companies began in a 2014 collaboration with a risk modelling company, RMS. RMS's clients are insurance companies who need to understand the financial risk exposure that comes with selling policies. RMS's commercial success in selling models for the new area of cyber insurance relied on implementing the Cyber Insurance Exposure Data Schema [**R2**] to identify impactful cyber scenarios and then quantify their business impacts [**R3, R5**], by accounting for the types and volumes of different policies sold.

This new cyber risk model was first launched in 2016 as RMS Cyber Accumulation Management System (CAMS), effectively licensing the CCRS cyber risk modelling framework for insurance analysis and accumulation control. The RMS cyber risk model is now one of the leading insurance and reinsurance models. RMS states that insurance companies responsible for 60% of affirmative cyber insurance licence their model, and this has resulted in USD3,000,000,000 gross written premium value. CCRS has partnered with RMS to produce annual updates to their model and regularly contributes speakers to RMS's client-facing seminars.

The RMS Chief Risk Modelling officer attributes much of these developments to CCRS:

'The CCRS is a leading centre of original research and creative thinking…it is no exaggeration to say that CCRS has played an important role in helping the insurance industry develop the cyber insurance market…The technical breadth and depth of the CCRS is truly impressive' [**S2** RMS].

The global defence and security firm Lockheed Martin has collaborated with CCRS on research into cyber risks including Cyber Resiliency [**S9**] and Sybil Logic Bomb [**S7**]. The latter introduced systemically important technology enterprises (SITEs) to describe companies whose products are so interlinked with commerce and society in general that their failure would cause problems on a very large scale [**S8** FT 2014]. Lockheed Martin's Director of Enterprise Risk & Sustainability states:

'*CCRS has been a valued research partner for Lockheed Martin in exploring cyber security threats...The Sybil Logic Bomb Cyber Catastrophe was one of the first to set out the potential for systemic impacts from a cyber-security incident and established the concept of systemically important technology enterprises (SITEs)… This research provided critical insights into the relationship between connectivity and cyber-security events. It also complemented customer relationship efforts and risk evaluation practices with suppliers*' [**S4** Lockheed Martin]

Cyber security is also a driver behind CCRS' relationship with the UK's terrorism insurer Pool Re, beginning in 2015 when the insurer identified cyber-terrorism as a key issue. The Chief Underwriting Officer at Pool Re highlighted both the value of collaboration with CCRS,

'*We quickly recognised CCRS as one of the leading thinkers in the emerging threat area of cyber and since then, we have worked together in understanding, quantifying and scoping the threat of cyber-terrorism*', [**S1** Pool Re]

and, in particular, the impact of CCRS' leading research in [**R4**]:

'Your report has proved particularly important in helping us to convince scheme UK stakeholders, including HM Treasury and other government offices, that our coverage should be extended. This puts Pool Re's over £6 billion funds under investment at the disposal of our UK policy holders in the event of terrorism event.' [**S1** Pool Re]

A similar model of direct engagement and collaboration with Lloyd's of London has provided direct benefits, including prescribing CCRS's scenarios as part of risk management reporting, attributing new insurance business being written in the Lloyd's market as a consequence, and ensuring consistency of data for cyber underwriting and aggregation management [**S3** Lloyd's]. Lloyd's Head of innovation remarked:

'CCRS has distinguished itself in its originality of research and its effectiveness in engaging with the insurance community. The exploration of systemic and emerging risks through developing and publishing scenarios has been highly influential in the insurance industry, which is increasingly dealing with new risks and business model challenges.' [**S3** Lloyd's]

On behalf of Lloyd's of London, the CCRS developed the 2015 Business Blackout report [**R5**] to address the prospect of a cyber-attack leading to large-scale power blackout. It has subsequently been adopted as a stress test scenario that all Lloyd's syndicate members must report on annually. Lloyd's Head of Innovation explains:

'*Lloyd's Business Blackout… This report has been extremely well received globally – we present material from it on a regular basis and the Lloyd's market uses the Scenarios as part of their Cyber Aggregation management process'* [**S3** Lloyd's].

Lloyd's was also both a driver and collaborator in developing the cyber risk data schema [**R2**] and it has become central in developing underwriting standards:

'*Cyber insurance exposure data schema… CCRS were very supportive of the Lloyd's Core data requirements and these have helped to encourage consistency of data for Cyber underwriting and aggregation management.*' [**S3** Lloyd's].

Lloyd's also provided funding for CCRS to develop a global City Risk Index, released in 2015, and update it in 2018 [**S10** City Risk Index] due to its commercial impact:

'*Lloyd's City Risk Index 2015-2025… The City Risk Index has raised the profile of multiple risk types globally and has led to new insurance business being written in the Lloyd's market as a consequence*' [**S3** Lloyd's].

The City Risk Index ranks cyber attacks 7th highest of all threats to global GDP [**S10** City Risk Index].

5. Sources to corroborate the impact (indicative maximum of 10 references)

Testimonials

S1 Pool Re Letter from Pool Re, Chief Underwriting Officer, highlights [R4]

S2 RMS Letter from RMS highlights [R2, R3]

S3 Lloyd's Letter from Lloyd's, Head of Innovation (Commercial Function), highlights [R2, R5]

S4 Lockheed Martin Letter from Lockheed Martin Corporation, Director of Enterprise Risk & Sustainability, highlights [R2, S7 Sybil Logic Bomb, S8 FT 2014].

Other sources

S5 Risk Summits: Cambridge Centre for Risk Studies, University of Cambridge https://www.jbs.cam.ac.uk/faculty-research/centres/risk/news-events/risk-summits/

S6 Taxonomy: Coburn, A.W.;, Bowman, G.; Ruffle, S.J.; Foulser-Piggott, R.; Ralph, D.; Tuveson, M.; 2014, A Taxonomy of Threats for Complex Risk Management, Cambridge Centre for Risk Studies, University of Cambridge

S7 Sybil Logic Bomb: Ruffle, S.J.; Bowman, G.; Caccioli, F.; Coburn, A.W.; Kelly, S.; Leslie, B.; Ralph, D.; 2014, Stress Test Scenario: Sybil Logic Bomb Cyber Catastrophe; Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge.
https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/technology-and-space/sybil-logic-bomb-cyber-catastrophe-stress-test-scenario/

S8 FT 2014, Financial Times, Tuveson, M.; Ruffle S.; 27 April 2014

S9 Cyber Resiliency: Kelly, S.; Leverett, E.; Oughton, E. J.; Copic, J.; Thacker, S.; Pant, R.; Pryor, L.; Kassara, G.; Evan, T.; Ruffle, S. J.; Tuveson, M.; Coburn, A. W.; Ralph, D. & Hall, J. W. (2016). Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy; Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge Judge Business School https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/technology-and-space/integrated-infrastructure-cyber-resiliency-in-society/

S10 City Risk Index: The Lloyd's City Risk Index, 2018, https://cityriskindex.lloyds.com/wp-content/uploads/2018/06/Lloyds_CRI2018_executive%20summary.pdf