Cyber Liability and Cyber Insurance: 
Analysis of the Chains of Liability Workshops 
London, 10-11 April 2019

INTRODUCTION

The Research Institute in Science of Cyber Security (RISCS) is the UK’s first academic Research Institute to focus on understanding the overall security of organisations, including their constituent technology, people and processes. RISCS is focused on giving organisations more evidence, to allow them to make better decisions, leading to the development of cyber security as a science. It collects evidence about what degree of risk mitigation can be achieved through a particular method – not just the costs of its introduction, but ongoing costs such as the impact on productivity – so that the total cost of ownership can be balanced against the risk mitigation that has been achieved. RISCS’s main goal is to move security from common, established practice to an evidence-based practice.

On April 10 and 11, 2019, RISCS held two workshops in London that looked at the complexities of liability in cyber insurance. We began each day with some presentations before embarking on the workshops. Topics covered in the presentations included the cyber insurance industry’s current state of play, and security challenges facing different sectors from regulatory, operational, socio-technical, behavioural, and business perspectives.

The purpose of Day 1’s scenario-based workshop was to explore the many forms of known, latent, and unknown liabilities that intersect with financial and legal chains of accountability. We also wanted to gain a deeper insight into where cyber insurance could provide a lever to promote a step change towards better cyber risk management. On Day 2, we took stock of the previous day’s findings in an interactive workshop to identify knowledge gaps and implications for future research.

We would like to thank all the speakers and participants for their time and input. In particular, we would like thank UCL STEaPP’s Digital Technologies Policy Laboratory for helping to design and facilitate the workshop. A special thank you to Sam B (NCSC) and Drs Ine Steenmans, Feja Lesniewska, and Kruakae Pothong whose inter-jurisdictional ocean-liner concept and transdisciplinary response elicitation methodology formed the basis of our workshops. We would also like to thank Katie E, Andrew F, and Peter Davies for providing valuable feedback during the preparation of this report.

For further information about this report or about other RISCS initiatives, please contact Emma Bowman at riscs.administrator@ucl.ac.uk.
METHODOLOGY

To create a complex problem space within which multiple disciplinary perspectives on liability issues in cyber insurance can collide and generate new insights, we gathered a group of 70 people from academia, industry, the policy community and the technical community.

As there is currently a lack of understanding about how risk, loss, responsibility and attribution may play out when the insured are faced with uncertain or perilous situations, the Day 1 workshop aimed to unpack the diversity of liability pathways using four hypothetical scenarios.

We randomly assigned the workshop participants to four interlinked scenarios in groups as shown below: 1. Man in the Middle; 2. Malware on Board; 3. Sickness Aboard; and 4. Tsunami Alert. The scenarios were underpinned by a common marine sector theme in which an ocean-liner is moving through different jurisdictions.

The escalating incidents in all scenarios exhibited both cyber and physical hazards with cascading effects and implications. Multiple actors were incorporated in the scenario-design, each of whom could partially be accountable for, and potentially be victims of, a series of adverse incidents that unfolded whilst at sea. Once the scenarios were presented to the groups for their reaction, the participants were asked to discuss the following questions:

A primary objective of the overarching questions was to scrutinise the participants’ view on the critical factors that shape emerging policy risks from cyber insurance and liability issues. These were often revealed through points of contention among the participants in various junctures of the scenarios.

The table facilitators were tasked with drawing these out of the discussions as much as possible. One of the tools at their disposal for this purpose was a subset of prompting questions (see Appendix A) listed under each of the four primary questions. The facilitators were instructed to inject them into the group discussions. The process was largely non-sequential and based on the facilitators’ discretion of the discussions’ trajectory and timing.

A spokesperson from each group was then asked to deliver a two-minute outline of their table’s scenario, accompanied by a one-minute summary of their group’s position on the questions above. Afterwards, the floor was open to inter-group dialogue to raise and exchange comments or questions regarding any of the four scenarios. Scribes were assigned to each group to take notes during the discussions and digitise them post-event. The notes were subsequently analysed to draw out the most relevant knowledge gaps identified and to articulate future research direction of RISCS.
DAY 1 WORKSHOP

1. Man in the Middle

The Scenario (Figure 1 below)
1. A man is a senior executive on a long-awaited cruise with his wife for their golden wedding anniversary.
2. He works in the telecommunications sector and his dealings see him in close contact with the many countries defence and national security apparatus.
3. Two years ago, he was accused by a foreign government of espionage during his time there on business.
4. He, like the other passengers, is using the ship’s Wi-Fi broadband service to talk to his family, browse the internet and send photographs to friends.
5. Half-way through the cruise, the ship unexpectedly docks at a foreign port.
6. A brief announcement is made shortly before making port, but the passengers are puzzled.
7. Within half an hour of making port, local police board the ship and are seen leading a man – the man – off in handcuffs. His wife is extremely distressed, as are many of the passengers and crew.
8. After a delay of 24 hours the cruise ship continues on its voyage.
9. His wife has disembarked and is staying in a local hotel.
10. He is imprisoned for a short time while extradition procedures are begun to send him to the country where he is wanted on charges of treason.
11. His lawyers are trying to find out how his whereabouts were known.
12. They do some research into the cruise ship company’s privacy policy.
13. It appears that while the ship’s broadband service is generally protected from snooping, it is subject to the laws pertaining to the country in whose waters it is sailing in at any time.
14. When it enters waters belonging to a few countries who insist on having the encryption keys for all encrypted traffic running over their radio spectrum, passengers are not alerted as “no one has ever historically expressed any concerns”.
15. In this case, however, the country in whose waters the ship was sailing appears to have been snooping on all traffic emanating from the ship to determine if he was on board.
16. At least, this is the only satisfactory explanation available to his lawyers.
17. This is reported in the press and many passengers still on board become concerned that their privacy was also breached without prior notification from the ocean-liner company.
18. The company is reported to the Information Commissioner’s Office, while his lawyers use this information in legal attempts to have him returned safely to his home country.

Discussion
A number of things were deemed ‘lost’ from the perspective of the couple and more generally, the passengers. Overall, these amounted to cognisable and non-cognisable losses for all involved due to feeling of vulnerability and, thus, an “inability to protect themselves.”

For the passengers and crew these included personal data, passwords, emotional distress, and consequential loss (e.g. missed connecting flights). The couple’s holiday and reputation were lost, so were the husband’s liberty and income and other financial costs that were incurred (e.g. alternative hotel arrangements for the wife; attorney for the husband).

The ocean-liner company also suffered some immediate losses such as its time, oil, encryption key (which has inherent value), and control over the ship. Potential losses projected down the line as a consequence of damaged reputation included the company’s future revenue, share price, and market position. Beyond the company, detrimental impact was envisaged for the whole sector as cruise ships...
were no longer be regarded as a viable choice for holiday escape – due to its subsequent association with ‘concerns like cyber security’.

The question of responsibility prompted more questions than answers. Although some participants suggested that the man, if guilty, should have been responsible for interrupting the cruise in view of his expertise in telecommunications. However, a closer inspection revealed this stance as problematic. An exemption from responsibility could be argued on the grounds that it was not unreasonable for him to ‘switch off’ to these matters during his holiday, including being caught unawares entering into a hostile port. Others noted that in principle, ‘blaming the user’ was not considered good practice.

Whilst the ocean-liner company failed to notify the passengers and crew, several factors complicated the situation. Firstly, two questions required further scrutiny: from whom did the company take advice during decision-making, and who made the decision to hand over the encryption, the cruise ship company or the telecommunications company? Other factors included the privacy policy concerning the company; the data sharing provisions of the jurisdiction within which the ship operated; whether the passengers were from the EU and the applicability of GDPR. The jurisdiction issue has further implications from a regulatory perspective: should the case be brought to the Information Commissioner’s Office (ICO), the United Nations, or other bodies?

Figure 1. The Man in the Middle scenario worksheet depicted with three contested points

![Man in the Middle worksheet](image)

Relatedly, the Captain’s responsibility over his decision to dock the ship was debated. More information and clarity were needed before it could be established whether he was at fault. For instance, what guided his decision-making process? What were the reporting lines for his decisions? Where did his instructions come from? Did he actually have a choice?

Further, as to whether any of this would change at all if cyber security was taken out of the equation, no consensus was reached. An example provided pointed to a US agreement with the EU and other jurisdictions to share passenger data on US-bound flights 72 hours in advance of the flight.
A mishmash of legal actions was put forth by the participants, which included a number of compensation lawsuits by and against different parties: the man/wife to sue the ocean-liner; class action lawsuit in California against the ocean-liner company and the man; the equipment company and the telecommunications company should be sued.

As a caveat to the suggestion that the passengers and the cruise ship company should file insurance claims, it was agreed that insurance companies should only intervene after responsibility and liability have been established. The underwriters should also be called upon for those facing lawsuits.

Beyond these attempts at individual and collective redress, all acknowledged the need for sectoral and investigatory response from regulatory bodies such as the Port Authority and the ICO. On the one hand, it was not immediately clear what the government or the embassy of the man’s country of origin could do to help him, though diplomatic complaint or sanction imposition were considered as viable options. On the other hand, the Foreign and Commonwealth Office should issue ‘cyber travel alerts’ that includes sections on ‘safe internet connection’ and ‘risks to data’. The government should also help share a list of countries or jurisdictions that require the sharing of encryption keys.

A battery of questions and comments were raised about what factors would determine the trajectory of how the case would unfold and its outcomes for those involved. The key question for establishing liability was ‘Why was the cruise ship in those waters?’ Other notable points included the decision making behind port docking and the encryption key hand-over.

The passenger’s level of knowledge about the risks of data sharing and encryption policy of the countries they were travelling through would have undoubtedly affected the outcome. The fact that the husband used the Wi-Fi made the cruise ship company part of the data breach.

Prior knowledge of the man’s ‘wanted’ status by the ship operator could have affected their decision to allow him to enter a different country. Such terms and conditions as well as other privacy policy of the cruise ship company were important to how the lawsuits would play out in the claims and judicial processes.
2. Malware on Board

The Scenario (Figure 2 below)
1. During routine administration of an ocean-liner’s IT infrastructure, an IT specialist receives an email and opens an attachment purporting to be an emergency Windows patch.
2. The IT specialist only recently joined the ocean-liner and was yet to receive training on cyber security procedures for the company’s systems.
3. Unfortunately, the attachment is malware.
4. Problems are quickly encountered throughout the ship.
5. Workstation consoles keep rebooting, and within a couple of hours some navigational mapping systems go offline.
6. Restaurant menu selection systems are also affected, and passengers begin to complain of not being able to connect to Wi-Fi.
7. The ship’s crew are having to default to contingency procedures, manually taking food orders, and constantly re-adjusting lighting and air conditioning by hand.
8. More seriously, though, the captain is navigating blind and is relying on a sat phone for weather and traffic updates.
9. The ship is 700 miles out to sea and while company bosses have advised the captain not to disclose the root cause to the crew, the captain is seeing increasing distress and unrest among passengers - including demands of a refund - and fears he will have to disobey orders while the ship is diverting to an island some 16 hours away.
10. The island is not well populated and there is no guarantee there will be the relevant expertise on hand to decontaminate the computers.

Discussion
A gradual but steady loss of control of all IT and physical systems was the overriding concern. The escalating consequences led to diminishing integrity of processes for risk management and quality assurance. On the people front, levels of trust, confidence and communication were eroding. The ship operator and its affiliate organisations faced financial and reputation losses, and the individuals on board faced increasing prospect of loss of health, safety and wellbeing.

Tensions heightened among the participants during the discussion around responsibilities. Clashing viewpoints emerged. Apart from the culpability of the perpetrator who sent the malware, antecedent responsibilities potentially lied with the IT specialist who opened the attachment; the person who trained the IT specialist; and the network architect who built vulnerability into the infrastructure.

Upstream the supply chain, segmentation in software for procurement could also have left a gateway open for undetected malware to enter.

The existence of prior knowledge about the malware vulnerability as well as any precautionary measures that should have been undertaken were regarded crucial to the attribution of responsibility retrospectively. It is important to find out whether risk assessment was carried out to evaluate risks to both IT and the voyage route. To do this, effective communication between security personnel, individuals performing the actions, and the decision-makers overseeing resources was seen as a must.

The process for determining proactive responsibilities in response to the incident was also questioned. Should the chain of command start with the captain or should the ship company take charge through instructions to the captain? Does maritime law apply here? Is there a protocol for manual navigation? Liability may partially lie with those providing direction from the satellite phone.
Participants discussed a range of immediate and latent actions. If there is incident management capability on board, the problem should be identified and isolated to understand the source of the attack, and forensic evidence should be collected and protected. The captain should take stock of any potential malware-related risks that might affect the ship, and ‘start an inventory of provisions to anticipate worst case scenario’. The ship company should contact other ships that may be facing the same malware threat to alert them to the situation.

Other concerns following the securing the immediate surroundings include requesting military support to protect the ship against piracy or in case of entering foreign waters. Logistics and supply chain considerations are required to manage the worsening of the situation’s fallout, such as further delays to the ships relative to their previously scheduled routes and tasks at the next destination.

If insured, the insurer has a pivotal role in the immediate aftermath and should be contacted to see how they may be able to help by providing expertise that is lacking on-board. That said, the extent to which the insurer could provide assistance is uncertain. However, the participants came to a unanimous agreement that all passengers on board should be entitled to compensation.

Public relations management measures such as press release, whilst important, may not be in the shareholders’ interest. It should nonetheless be on-hand and ready for publication if the breach or compromise becomes widespread.

It was clear that an internal review should be undertaken and complemented by an independent external review to validate the findings, the latter of which may prove valuable for the board of directors.

Uncertainties revolved around the question of which authority should arbitrate compensation claims. Several factors could potentially dictate this: the jurisdiction of the ship company; the jurisdiction that was stated on the insurance legal contract; the waters and jurisdictions that the ship had sailed through; and the jurisdiction of the island on which the ship came to a stop.
3. Sickness Aboard

The Scenario (Figure 3 below)

1. An ocean-liner enters a regional Sea on its way to a popular tourist location near a historic port city.
2. During the cruise, two passengers have become infected with what is thought to be pneumonic plague, a highly infectious influenza-like illness (ILI).
3. Following international protocol the ship’s doctor has confined the two passengers to their quarters and quarantine procedures have been invoked.
4. The ship’s doctor also informs the Centre for Disease Control and Prevention (CDC) that two passengers have contracted an ILI.
5. The next step is to proceed directly to the nearest port to arrange medical transportation of the two patients requiring hospitalisation upon arrival.
6. The ship’s captain is about to make a telephone call to the port to request an emergency landing.
7. Meanwhile, a national security agency (NSA), informed by the CDC of the situation, has been conducting a cyber intelligence review using the ocean-liner’s online activities to get a more accurate picture of the situation on board.
8. It conducts the intelligence review without making direct contact with anyone on board the ship or the cruise ship company headquarters.
9. Using big data analytics the materials gathered – partially undertaken by AI – it appears that the plague outbreak on board the ship is out of control, with many more cases than have been officially reported by the crew.
10. The CDC inform the port authorities on the small island states nearest the ship’s current location and issue advice to refuse requests for landing.
11. The Port Authority that the ocean-liner’s captain has contacted make an emergency decision to allow landing but prevent disembarkation of passengers until the facts are established definitively.
12. Disembarkation for all passengers and crew is delayed by 96 hours until the ship’s captain reports to the CDC a further three passengers are showing flu-like symptoms and the two initially quarantined have died.
13. Medical personnel are immediately deployed onto the ship to assess the situation.
14. It emerges that the captain’s original reports were correct.
15. This prompts a decision to allow disembarkation of all remaining passengers and crew.
16. The delays to disembarkation caused the needless death of two passengers.
17. Angry family members turn their attention to the small island Port Authority.
18. The Port Authority however blames the intelligence received from the security agency.
19. The agency refuses to disclose information on grounds of national security.
20. Meanwhile there is high profile public attention on the incident.
21. The Cabinet Office begins deliberating on next steps and issues an interim ministerial press statement.
22. They have been briefed by the agency responsible for informing the port authorities, and it appears one of the data feeds they used was based on metadata from a large social media company.
23. Early indications are that hits on the keywords “flu” and “plague” coming from social media users located in the general area of the ship were unusually high.
24. The AI’s interpretation was that there were numerous instances of the disease in that area.
Discussion
The loss of two lives in this scenario, without a question, trumped all other losses incurred. Even if the victims had appropriate life insurance coverage and their family members were compensated financially, the participants perceived no gains for anyone ultimately. At a distant second to the lost lives were a loss of trust in the information system and the cruise, and reputational loss for the company.

At face value, the cruise ship appeared to be responsible for the disastrous outcome. However, the question of ‘What else could the cruise ship have done?’ quickly showed that the idea of a single party being primarily responsible was far too simplistic. The chain of events required unpicking to appreciate the degrees and ways in which all actors were responsible. It became clearer, as a heated debate ensued, that deflections of blame were highly likely to occur. To gauge how different parties would protect themselves from accepting liability, a finer look at how risks and responsibilities may have shifted along information channels and decision-making chain is needed.

One fruitful way to proceed with this, agreed by all participants, was to establish clarity around communications protocols between the government agencies and actors on the ground. Inevitably, the cruise ship would be subject to wrath from all sides as a result of efforts to deflect blame and pin guilt, including its portrayal in the media. In spite of this, as the authorities, the CDC and NSA also bear responsibility but at a higher level for operating a broken system.

On the technology front, more information is needed about big data and AI technologies. Although the false claims made by the passengers on-board could be considered an illegal action that misled the NSA’s analysis, the underlying issue here points to a cultural shift of a heavier reliance on technology data rather than the physician’s expert knowledge. This proved deeply concerning because a tangible report based on trustworthy information was dismissed in favour of an AI report derived from unverified data sources.

Figure 3. The Sickness Aboard scenario worksheet depicted with three contested points
Since the cruise ship operator was at the mercy of the unfolding incidents and had very limited options during the incident, the discussion around actionable items was mainly centred on redress options and potential improvements at the strategic level.

For instance, preventative measures the cruise ship should take include having contingency plans and better communication procedures in place. Companies can conduct a ‘lessons learned’ session and look into arrangements to employ private helicopter during emergencies. The NSA needs to ensure that the data sources can be trusted, which includes manual confirmation of AI-generated results.

‘A chain of lawsuits’ was regarded as an appropriate redress option. The participants agreed that the victims’ families and the cruise ship company should sue the government. This would pressure the government into taking action whilst potentially allowing the families to collect insurance pay-out – assuming that the government was insured. Then, once the families won their lawsuits against the others – with the help of the insurance company to show that the government was indeed negligent – the insurance company could recuperate the monies paid out. It was caveated, however, that the legal concept of sovereign immunity would make suing a government extremely difficult.

One of the key lessons learned from this scenario was that solid evidence-base should be prioritised in decision-making over flimsy technological solutions. To make this work, good judgement is needed in differentiating information types and data sources, and how best to weigh their relative trustworthiness. To enhance these processes, the challenging tasks of identifying the decision-making points and the actors behind them need to be tackled. An awareness of the political element in the unravelling of such complex situations would be required.
4. Tsunami Alert

The Scenario (Figure 4 below)
1. An ocean-liner is sailing the Ocean carrying a full complement of passengers.
2. An early warning system designed to alert crew to tsunamis generates a text alert.
3. The captain sees the text alert and in response diverts the ocean-liner’s course away from the path of the tsunami.
4. In fact, the ocean-liner actually sails into the tsunami’s path.
5. The ocean-liner sustains major structural damage and 18 passengers and crew lose their lives.
6. Survivors are rescued by a helicopter that is dispatched by the nearest state’s Sea and Coast Guard Agency.
7. Families of the dead and injured initiate proceedings for a class action against the ocean-liner company claiming manslaughter by negligence.
8. Two months later the company retrieves the ship’s black box and hand it over as digital evidence to the National Transportation Security Board – considered a competent authority in these matters.
9. The investigation is conducted in secret, although periodic press briefings are held.
10. Stories apparently leaked to the press suggest the captain responded in good faith to data received from the early warning system but that the data was partially incorrect and transmitted in a language the captain was not fluent in.
11. The ocean-liner company deny wrongdoing and are allegedly making moves to sue the local agency responsible for transmitting the early warning information.
12. Meanwhile the agency blames publicly known data issues associated with the operational use of the early warning technology itself.
13. There appears to have been little or no training provided in the operational usage of the system or the response procedures.
14. The cause of the tragedy appears to revolve around a complex supply chain which no-one fully understands.

Discussion
A delineation between tangible and non-tangible losses was drawn. The former included loss of life, equipment, revenue and damage to the ocean-liner, insurance compensation, the holiday, and other consequential financial costs including those associated with the rescue mission.

The non-tangible category also encompassed personal losses stemming from the loss of life, but also the survivors’ loss of abilities as a result of the injuries sustained. Further, trust is lost in the cruise ship company (along with a loss of reputation), the tsunami warning system, the whole supply chain of this service (e.g. manufacturer, operator, data collection and processing), and the National Safety Board’s non-transparent procedures.

Just as the responsibilities do not reside with any single individual but are shared, the same applies to the ownership of risks. Moreover, certain legal considerations such as strict liability and contractual responsibility are already in place and commonly used to determine and guide insurance coverage and compensation lawsuits. Whereas strict liability applies to the captain and the crew, contractual responsibility implicates the tsunami warning agency and the manufacturers of the tsunami warning devices and analytics due to ‘implied capabilities’. Unless caveated in the contract that the early warning system may not be 100% accurate, by precedent or reasonable expectation, it would have needed to provide precise instructions to eliminate responsibility.
Further, the outcome of the insurance claim may vary depending on the contractual terms’ minutiae and the circumstances surrounding the adverse events. The following questions were deemed relevant to ascertaining where and with whom responsibilities lay:

Issues relevant to the captain and crew:
- Was the insurance for the role of the crew or the person?
- Could the insurance say that we are not insuring you because we insure the person?
- Was the captain an employee of cruise ship company or subcontracted?
- Does the captain’s contract state his responsibilities?
- Was the captain certified? Did the role have language requirement? If so, which language(s)?
- Should the training have included a wider scope?
- Should the contents of the text message have been controlled?

Issues relevant to the systems and captain:
- What is this system?
- Was the ship leased to the cruise ship company?
- What device was the text message delivered to? What was the message for them?
- What was the compatibility of systems used for sending and delivering this text message?
- Was the early warning system designed to protect ships or people on the coast?
- Was this system misused?
- Should the captain have checked whether they needed to act? Were actions taken simply because they believed a response to the warning was needed?
- Did the captain act responsibly? Was the captain in complete control of their faculties?
- Did someone hack the ship to make it not do what the captain told it to do?
- Did the instruments malfunction and indicate that the captain has solved the issue when in fact they have not?
- Did the company check the license?
- What were the country requirements for training?
In hindsight, preventative steps could have been taken to provide the right level of support and awareness. The ocean-liner should have ensured adequate training for the captain and the crew and created a feedback loop. The warning system should have been designed to support situational awareness. Part of this involves diverse intelligence support for the captain based on satellite imaging, weather forecast and special radar for detecting obstacles. Notwithstanding these, the captain should also not have relied solely on one source of data and information.

Business decisions need to be made regarding whether to overhaul the market approval system of the early warning system, and, although costly, whether to recall all other early warning systems that are already on the market.

Following the incident, an independent regulatory body should produce a root cause analysis of the incident and make the report publicly available. Findings from the report should provide guidelines for new standards and learnings for all stakeholders. While it was clear that investigations should be opened into the captain, the ocean-liner, possible tampering with the systems and hacking, and potential harm caused by benign insider, basic questions remain as to what kind of investigatory and legal processes would be appropriate. Questions such as who should arbitrate, what kind of arbitration, in whose court, and which waters and jurisdiction all need to be determined prior to taking further actions.

As one of the determining factors in the case, the question of ‘Is it an act of God or not?’ led to vehement disagreement without resolution. Another question pertinent to the heart of the issues raised in this scenario was: ‘Why knowing the potential safety implications did the captain act on the uncorroborated evidence of a single sensor/ information system?’ Finally, a range of other factors that could be used to determine whether to take someone to court, and also in court for determining liability, were discussed as shown below:

- Technology: The accuracy of the warning system’s sensing devices and data analytics.
- Data: The accuracy and integrity of the data and the system.
- Captain’s experience and actions: Ability to interpret and understand the data and system, and to discharge duties in the face of (increasingly) complex systems.
- Crew’s experience: Whether procedures were followed in this incident, and whether they understood the responsibilities in the training.
- Other factors: Over-dependence on technology; false trust in the system.
Future Research Direction

As the event drew to a close in the final plenary, the participants shared the knowledge gaps that they identified throughout the proceedings and exchanged ideas about pressing concerns that needed to be explored further through research.

To inform future research direction of RISCS, we carefully curated the findings from the workshops and the knowledge gaps identified. Specifically, we looked for research themes and questions that were salient not only to cyber insurance and cyber liability issues, but also to developing a better understanding of cyber security through an economics and incentives lens. Finally, these themes and questions were used to shape a new Call for Research Proposals due to be launched in early 2020.

Theme 1: Economics & Market design
- What (emergent) practices, business models, behaviours and relationships characterise the national and international cyber security market?
- What type of informational mechanisms or cultural considerations are required for the cyber security market to function optimally?
- How can current market design aspects in cyber security be optimised (e.g., feedback loops, metrics, eliciting ground truth, contractual language, cultural factors)?
- What product portfolios are currently missing but may be urgently demanded within the industry from the insurance sector? Are there any gaps in what insurance firms can cover? Given information asymmetries between the insurer and the insured, how can this be improved?

Theme 2: Incentives & interventions
- What measurable consequential effects have been derived from previous cyber security interventions and incentives in the UK?
- What would be the effect of potential future interventions to enhance cyber security and secure behaviours on UK cyber security?

Theme 3: Data & modelling
- What types of data could be collected to help better model cyber security risks more accurately?
- What is the level of preparedness and the scale of accuracy of current risk modelling? For instance, what is the understanding of the distribution of events and modelling of long-tail events?
- How can the level of exposure and risk across the cyber insurance customer base be minimised?
- What are the chains of risk ownership and the extent of liability the market has to address?
Theme 4: Effect of cyber insurance on secure behaviours

- What measurable, longitudinal effects does cyber insurance have on avoiding moral hazard?

- What positive outcomes of cyber insurance can be enhanced and championed to direct and guide secure behaviours?

- What lessons can be gained and behavioural models can be applied from other sectors or other insurance portfolios that positively change behaviours?
APPENDIX A: PROMPTING QUESTIONS

Same for all four scenarios

WHAT IS LOST?  This is to help attendees reflect on the nature of risk.

- What is the loss?
- Loss of life, finance, reputation, data, ...?
- Who owns the risk?
- Who is benefiting?
- Who has financial gain?

WHO IS RESPONSIBLE?  This is about exploring attribution: who is responsible?

- Who is trying to deflect responsibility?
- Is there a mismatch of who is responsible and who is liable?
- What complicates attribution?
- Should an individual be held responsible? Or an institution?
- Is there a behavioural dimension?
- Are there different capacities by individuals to handle this?
- Where could there be injustice?

WHAT ACTION SHOULD BE TAKEN? BY WHOM? WHERE?  This is about exploring how this scenario could be handled by regulators, insurers, government, etc.

- What is appropriate action here? Insurance claim, arbitration, court, ...?
- Who should arbitrate?
- How should they arbitrate?
- What information that you did not get in the scenario would you have liked?

WHAT IS A DETERMINING FACTOR IN THIS SCENARIO?  This is about understanding what the critical issues are that influence the narratives on law and/or liability.

- E.g. Jurisdiction, citizenship, interstate agreements, etc.