Supplementing Cyber Risk Discussions with an Actuarial Perspective

The incidence of major cyber events making international headlines on a regular, and increasingly frequent, basis has seen cyber security rise to the top of many companies' agendas over the last few years; cyber incidents have been cited as the clear winner of Allianz's Annual UK Risk Barometer for the third consecutive year.

With well-publicised cyber-attacks ranging from those where the indiscriminate and geographical reach of cyber took the world by surprise (Wannacry, NotPetya) to those with significant financial/reputational implications (TalkTalk, British Airways), dealing with cyber security is starting to become a question framed as how to protect against losses *when*, rather than just *if*, an event occurs.

Unfortunately, despite the increased awareness of cyber security matters in recent times, risk management practices have struggled to match this trend. The Cyber Security Breaches Survey 2018 is an official statistic which looks at how UK organisations are approaching cyber security matters. The 2018 survey found that, although 74% of business categorised cyber security as a priority for their organisation's senior management, only 27% of businesses had a "formal cyber security policy or policies".

Why then, has the increase in board-level appreciation for cyber risk not resulted in tangible actions in the form of cyber security policies and strategies?

Current Risk Management Practices

Adopting best practices such as ensuring software updates take place, configuring firewalls, the use of safe password practices and multifactor identification are necessary but certainly no longer sufficient when it comes to protecting against cyber risk today. Companies need to ensure that they are assessing and addressing cyber risk adequately; for example, this may be through effective response planning or penetration planning.

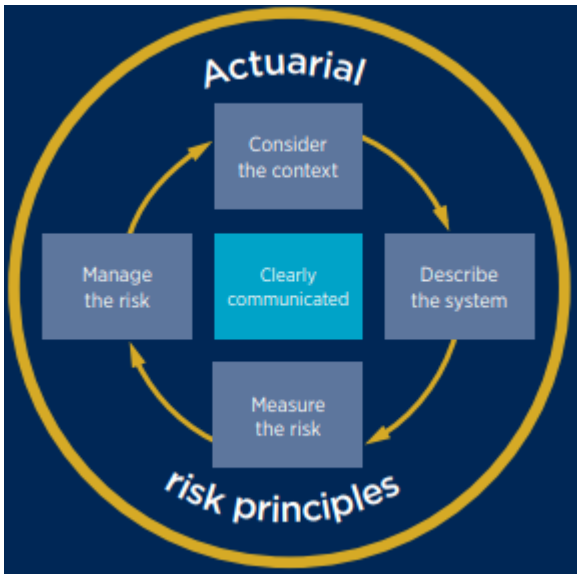
An obvious part of the reason behind any current risk management deficiencies may be due to the challenging business conditions. Cyber risk management is limited by budgets set aside to deal with the risk as well as the level of access to adequately trained resource an entity has.

Another explanation may be that executives have insufficient knowledge of the threat landscape to make effective decisions relating to cyber security policies and budgets. Cyber-attacks come in many forms (e.g. malware, phishing, DDoS, MitM) as do potential losses (e.g. incident response costs, business interruption, regulatory fines). It may be this variation coupled with the ever-evolving characteristics of the cyber world, with its increasing number, loss amounts and sophistication of cyber-attacks, that acts as a further hindrance when developing meaningful cyber risk management.

There are a number of standards available which can assist with cyber security; the NIST Cybersecurity Framework and ISO/IEC 27001 to name just a couple. These standards offer best-practice information and controls which can be implemented in an organisation to help with preventing, detecting, responding and recovering from cyber-attacks. However, the in-house use of such standards also requires resource allocation, and, for some companies, Boards may need to be convinced prior to additional budget being allocated.

Actuarial Risk Principles

Dealing with emerging risks is something that actuaries are experienced in and well equipped for, which makes cyber risk management an area where actuaries are starting to add value. A general summary of an actuarial approach is captured by the ***Actuarial Risk Principles***, which were launched by the Institute and Faculty of Actuaries (IFoA) last year. A cyber risk case study was also considered at the time, and the reader is directed to the references for further details.



The diagram shows a simplified version of the framework that actuaries use when dealing with risk management. Such a framework can help to add value, particularly in the case of a situation where there is uncertainty as is the case when faced with the evolving cyber threat landscape.

Considering the context, with the potential for cyber events to generate significant financial losses, organisations need a robust analysis of what could occur and what their options would be.

This is also an area which the IFoA's Cyber Risk Investigation working party has been working on. The working party propose a framework, based on the NIST framework and the cyber risk CRO Forum Concept Paper, with which to develop cyber operational risk scenarios.

In particular, the working party will soon be releasing their sessional paper which includes three worked examples ***describing and measuring the risk*** using the proposed framework; these examples include detailed breakdowns of the various potential sources of losses, associated approximate loss amounts (and rationale behind any figures) as well as potential mitigation options.

The value of different approaches to ***managing the risk*** will clearly vary depending on the entity and the specific risks involved but the paper provides useful food for thought; examples range from "good housekeeping practices" such as electronic monitoring and network security to other more sophisticated considerations such as pro-active security intelligence gathering.

The value in purchasing a cyber insurance policy should also not be underestimated since, even in cases where entities have relatively robust cyber security/risk management practices, there will always be residual cyber risk. As with any insurance contract, care should be taken to understand what cover is being purchased and which exclusions are in place.

It is through the development of such detailed and tailored cyber scenarios that we can illustrate cost-benefit analysis of mitigation approaches and start to bring board-level cyber risk discussions to life. With the cyber landscape advancing at such a rapid pace, work must be done to ensure that cyber risk is ***clearly communicated*** and given the attention it demands when it does appear in front of executives and other business decision making personnel. This will help to not only drive awareness for the scale of cyber risk exposure but also help companies to identify where any vulnerabilities in cyber security policies lie so that actions can be taken before a company faces a cyber-attack rather than in the aftermath.

References:

Actuarial Risk Principles: https://www.actuaries.org.uk/news-and-insights/public-affairs-and-policy/evolving-risks-and-future-insurance/actuarial-risk-principles

Cyber Risk Working Party: https://www.actuaries.org.uk/practice-areas/risk-management/risk-management-research-working-parties/cyber-risk-investigation

Jasvir Grewal is a general insurance actuary working at Arcus 1856, which is a Lloyd's syndicate backed with funds managed by Credit Suisse's ILS team. She holds a master's degree in Mathematical Modelling and Scientific Computing from the University of Oxford and is a Fellow of the Institute and Faculty of Actuaries (IFoA) as well as a Chartered Enterprise Risk Actuary. Jasvir has several years of actuarial experience, particularly in capital modelling. She has a keen interest in cyber risk/risk management and has been involved in several IFoA working parties.