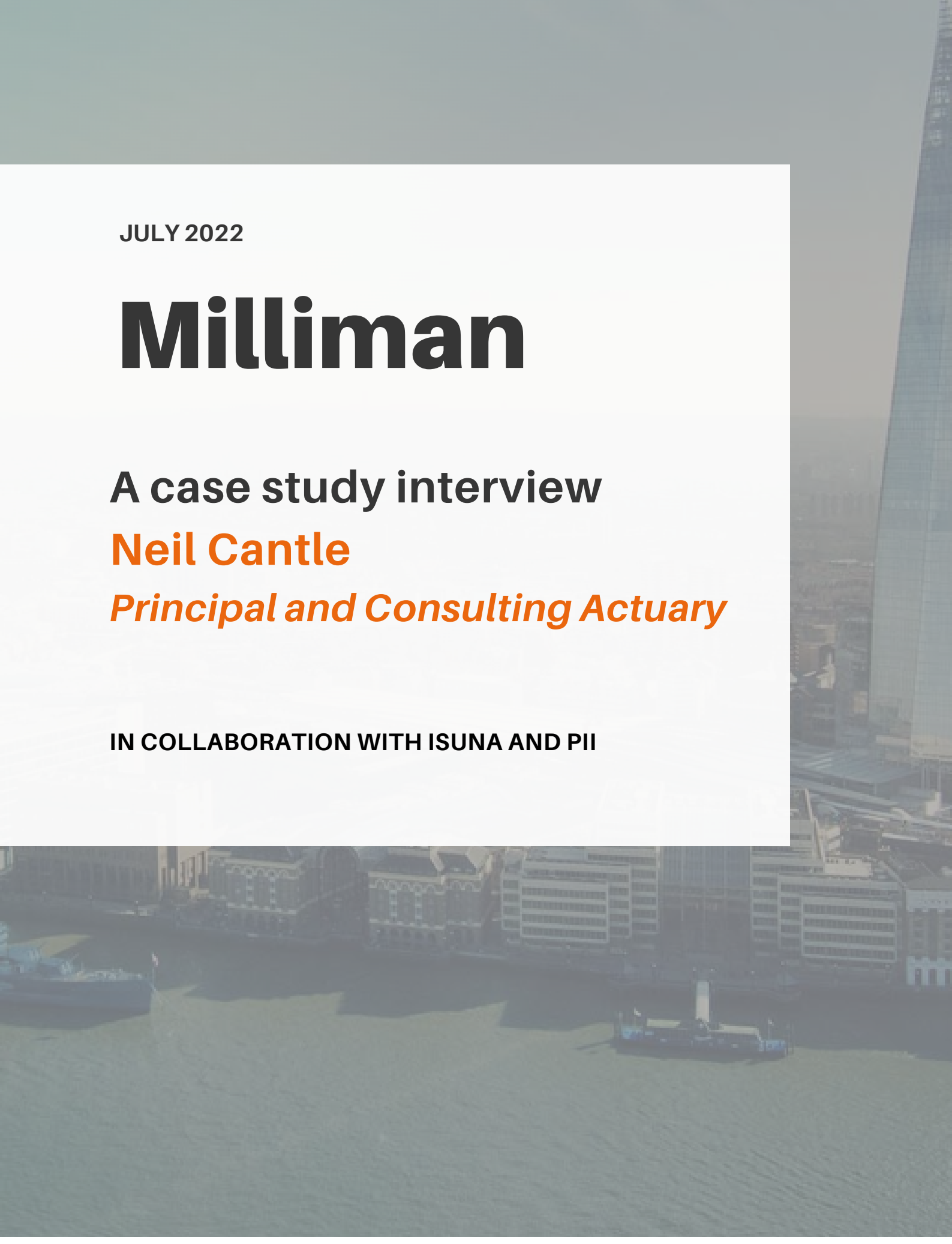


JULY 2022

Milliman

A case study interview

Neil Cantle

Principal and Consulting Actuary

IN COLLABORATION WITH ISUNA AND PII

iSUNA

PEACE INNOVATION INSTITUTE
THE HAGUE

Milliman

Milliman

Milliman is a global actuarial and consulting firm operating with 59 local offices that focuses on helping people and companies solve financial problems.

This largely involves risk management and predictive analytics. Main client industries target a number of insurances and healthcare. With the rise of cyber insurance, Milliman is increasingly growing its reputation as a key stakeholder in the cyber industry as they provide consulting services for both cyber insurance companies, helping them to understand the cyber risk they are insuring, and exploring the factors that drive more accurate pricing. Also, to support companies who are trying to understand their own cyber exposure, exploring the risks businesses take, what cyber exposure they have, and how that exposure behaves. Herein, Milliman works at the intersection between the insurer, and the (potentially) insured providing a high-quality international pool of information and data enabling cutting edge predictive analytics for the cyber industry.

Neil Cantle

Principal and Consulting Actuary at Milliman UK

In this interview, we were lucky enough to speak with Mr. Neil Cantle from the London office at Milliman. Neil has spent over 20 years in risk management and over 30 years working in financial services. His role as Principal and Consulting Actuary regards work in risk management, and senior risk roles. As a recognized thought leader in risk management, Neil led the global development of the CRisALIS™ methodology, comprising techniques in social sciences, complexity sciences, and AI.

www.uk.milliman.com

www.linkedin.com/in/neil-cantle

A unique approach

Cybercrime occurs at any given time, in multiple places at once. The scaling of cybercrime in the past decade has made it an adversarial sector that continuously adapts to overcome the latest cyber security protection functions, and cyber security protectors adapt to the techniques employed by cyber criminals. This back and forth between the two actors occurs far more often than the financial review period of a protected company, every 12 months. Far quicker turnover times for this review are necessary in order to take adequate actions against cyber threats.

To overcome this, Milliman has built an approach that can be conducted as frequently as desired and that is agnostic to the type of company. This means, the approach for the IT department of a military organisation for example, who is being hacked every five minutes receives a different approach than a smaller company with a lower risk profile, such as a sales team. Additionally, the approach by Milliman is encompassing perspectives beyond historical financial data, and rather begins an analysis from understanding what is really going on at the ground level of the company.

CRisALIS™ - A Three Step Process

This approach is the CRisALIS™ methodology; a cutting-edge approach developed by Neil that explains and models complex risks, such as cyber, faced by an organization. This intends to measure points of subjectivity and quantify them to predict risks. In a three step process CRisALIS™ starts by exploring the subject matter expertise of the event, then approaches a data challenge, and finally creates a prediction.

CRisALIS™ - A Three Step Process

This approach is the CRisALIS™ methodology; a cutting-edge approach developed by Neil that explains and models complex risks faced by an organization. This intends to measure points of subjectivity and quantify them to predict risks. In a three step process CRisALIS™ starts by exploring the subject matter expertise of the event, then approaches a data challenge, and finally creates a prediction.

1. What you know

For example, cybersecurity of an IT department; through hosting a workshop with interviews, the proposition of the entire department are extracted in plain language. This explains the workforce culture, behavior and outcomes that could possibly expose vulnerabilities of the cybersecurity practices in that department.

One example here could be exploring how well the team understood the dangers of phishing links and how to be cautious, instead of seeing in their records whether the team checked the box for completing a cybercrime prevention course.

This informs a deeper and more credible understanding (yet still presented simply) of the organization and helps uncover a narrative that may be traditionally glamorized in the form of certifications, green check marks, and standards met. There is always more to be seen.

Social science techniques are applied to analyse the rich collective narrative obtained from the experts and then reduce it to a minimally complex form. This enables the key features of the situation to be easily understood.

2. The data challenge

This becomes the second step in the process, with the qualitative constructs, Milliman compares them with historical data to raise the challenge of what is known and what is seen. It becomes a tense comparison of exploring the model of assumptions that might be known by subject matter experts and actuaries, but it may not be present in that data. On the other hand, factors unknown to the experts and actuaries may be present in the data, and then decisions need to be made on whether those factors are relevant. This is where complexity sciences makes an appearance.

By looking at the data Milliman explores the relationships using information theory and transfer entropy, to help identify possible triggers for slow moving change that could have a cascading effect once a tipping point is reached.

3. Developing the Prediction

The final step is to make the prediction using a Bayesian approach. The development of a causal model is calibrated to a condition that is parallel to what happens today, to predict what may happen in the future. This is where assumptions and advices are made to best place an investment to reduce risk that would have catastrophic consequences. Given the baseline of the state of the workplace from the initial step of expert input, and the goals set by board teams of where they want to be, Milliman can use predictive modeling and analytics to navigate best placed investments to safely steer the organization.

Overall, these three steps enable the CRisALIS™ to utilize plain language explanations that can then be embedded into a model where relevant factors are analyzed to advise the best places of investment to reduce risk. These judgments rely on both the opinions of expertise and the actuary in an attempt to integrate what has happened in the past, but also what you predict will happen in the future.

In different parts of the world, different organizational cultures exist. In the application of cyber insurance and cyber security, the risk for cyber crime consequences will increase or decrease on a basis on the culture of the organization, which is dependent on the culture it resides in. To overcome culturally-sensitive translation issues, Milliman operates through locally based offices rather than regional offices. This allows for closer connections between actuarial consultants and clients to develop a more contextually sensitive model of the organization when utilizing qualitative metric techniques.

Interconnectivity and Complexity

Within the work of Milliman, denying the complexity of cyber activity and its relationship to organization and social function is not an option. Often relevant factors that may address the weaknesses of an organization can be overlooked when trying to simplify the reality. One example is the use of taxonomies, simplifying the reality of a cyber-attack as it categorizes the relevant factors often to one item on a risk register. While admitting the complexity is a large undertaking, in a systems view it opens a more accurate understanding that anything can happen — which is better than eliminating risks that could potentially happen.

Slow-moving change

In risk management, clients need clarity. However, there are a series of known factors with unclear outcomes. This can make the client feel uncomfortable. By examining these interactions as a series of interconnected systems and subsystems, it becomes possible to identify the impact of different factors at different speeds and scales within society. This concept is known as Panarchy, stemming from ecology. At the lowest scale, the individual business, the factors in question are frequently relevant. In the next larger scale, at the industry level, the factors are slightly less frequent but still noticeable. At the societal scale, those factors and their influence are almost unnoticeable. The societal scale change is moving so slow, that it becomes difficult to see whether those factors are relevant, or if they even exist. For example, when looking at two photos of a field of grass you may assume they are the same photo, even if they were taken two weeks apart. Only after showing a time lapse video of the grass growing is the change noticeable.

The world has known for over a decade if a pandemic were to occur, everything would fail. However, as no one individually saw the accumulation of risk factors governments and people chose to pretend it wouldn't happen rather than prepare.

Tools are necessary to understand the slow moving processes that are frequent at the individual business level, but harder to identify at the societal level. This is particularly important to recognize as once these relevant unidentified risks accumulate over time, when a catastrophic event occurs (such as the covid pandemic) all the risks occur and there is a rapid cascading effect disrupting the systems maintaining order. In cyber insurance, this is identifiable now where the accumulation of risks within businesses, and the dynamic nature of cybercrime has led to financial and non-financial losses to accurately provide insurance.

A means to discovering these slow-moving factors is through information theory. Milliman uses this in the CRisALIS™ methodology to identify the smallest factors, then with subject matter expertise and actuarial expertise, an educated conclusion is drawn on whether that factor may be relevant.

Bringing the future forward & Isuna

The world has known for over a decade if a pandemic were to occur, everything would fail. However, as no one individually saw the accumulation of risk factors (even though aware of the risk of the catastrophic event) governments and people chose to pretend it wouldn't happen rather than prepare. However, there is a fine line between being protected, and being overly protective. Here Milliman optimizes a systematic approach that is context dependent to help companies make the most impactful investments within their risk portfolio. This examines both the ways in which adverse outcomes can arise and the associated impacts as a connected concept within cyber, to identify the causal flows that originate within an adversarial space.

In convincing clients to take measures, Milliman tries to bring the future forward, presenting the clients with scenarios based on a qualitative and quantitative evidence-based risk assessment of what could happen.

At Isuna, taking account of the adversarial space is where our strength lies. As well as understanding that cyber protection is a process; a simple certification does not protect you against an attack. Through a system of consistently tracking progress companies are able to see the risks and strengths identified within their business to adhering to ISO and GDPR regulations. Here, the Isuna platform helps account for many risk factors beyond the ISO and GDPR embracing the complexity of cyber challenges in the business sphere.

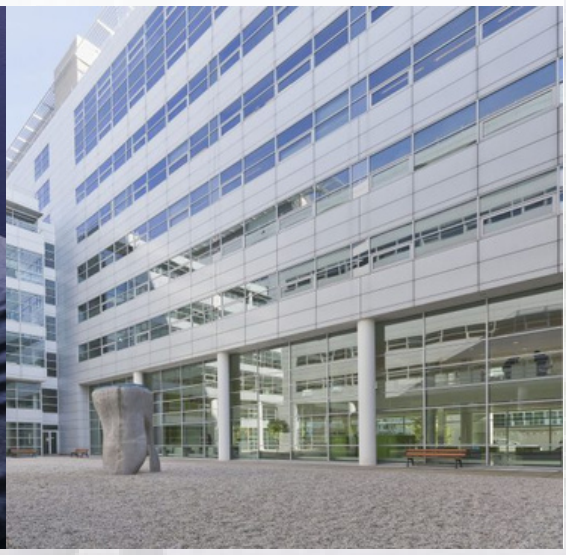
About Isuna

Isuna BV, based at the HSD Campus in The Hague is a company that focuses upon helping companies build their resilience to cyber threats and increase their awareness of the options that are available to them. To do this we provide Compliance Platforms that enable companies to effectively and efficiently implement regulations such as ISO27001 and GDPR (or AVG here in the Netherlands). We are trusted partners of Royal NEN [1] and recently validated by an EU programme. [2]

We have initiated a project to better understand the Cyber Insurance market and to connect stakeholders so that we can increase the accessibility, understanding and value to businesses. We are developing case studies, such as this one, to highlight approaches and to help the insurance sector build their services and collaborations based upon building market share through the provision of improved services. We will continue this work and look forward to sharing our analysis and research.

If you work within the cyber insurance sector and can provide some insight or want to be the subject of the next case study please contact us directly.

We'd like to thank Mr. Neil Cantle for his time and energy in providing us with his insights about cyber insurance and his expertise as Principal and Consulting Actuary at Milliman and in his leading role in the development of CRisALIS™.



1. www.nen.nl/isuna
2. https://www.kansenvoorwest2.nl/nl/nieuws/isuna-compliance-and-resilience-platform/

EUROPESE UNIE
Europees Fonds voor Regionale Ontwikkeling.
Mede gefinancierd in het kader van de respons van de Unie op de COVID-19-pandemie.
G4P4 Kansen voor West II