Risk.net

Paper of the Year: Embrechts, Mizgier and Chen

Embrechts, Mizgier and Chen expand operational risk modelling across industries

Paul Embrechts: “EVT gives you a way of thinking about non-normal data and that’s why it is important”

Risk staff

19 Jun 2019

It was once feared that the end of the Advanced Measurement Approach for operational risk capital, would mean the decline of op risk modelling – without the regulatory incentive to construct and maintain models, investment and interest would dwindle away. Instead, the reverse has been true, and the *OpRisk* Paper of the Year was a narrow first in a very crowded and competitive field.

At ETH Zurich, Paul Embrechts, Kamil Mizgier (now at BNY Mellon) and Xian Chen (now at the University of Oregon) used a model based on dynamic extreme value theory (EVT) to explore the links between internal control weaknesses and the severity of op risk losses.

Their paper, ‘Modeling operational risk depending on covariates: an empirical investigation’, was published in the ***Journal of Operational Risk*** in March 2018. It was the first use of dynamic EVT to link internal control weaknesses to severity rather than simply frequency.

Industry collaboration was the key to the research, which depended on the use of a 20,000-point loss database provided by the SAS Institute,

Mizgier asserts.

“Ten years ago, at UBS, we looked at dynamic operational risk models,” he says. “Thanks to my contacts in the industry, we could get access to the data, and this is the most important and difficult thing for researchers – getting reliable industry data. There has been a lot of theoretical work, but without data you can’t calibrate a model or make meaningful relevant insights.”

Not all of the loss data came from the financial sector. This allowed the researchers to carry out cross-industry comparisons – and also underlines the importance of op risk modelling for every industry, not just finance, notes Embrechts.

“It’s clear that operational risk is an issue way beyond the financial industry,” he says. “It became an issue [for them] with Basel II, Basel III, Solvency II and so on, but the data that we see is relevant throughout industry.”

Cyber is an area where new covariates are really having a huge influence and the model we propose is very relevant

Paul Embrechts, ETH Zurich

Although operational risk losses in finance tend to receive the most attention, loss severity is actually significantly greater in manufacturing, reflecting the greater investment in physical plant.

“It’s important to look at this in order to measure and regulate it,” Mizgier says. “Financial services are more regulated, so the losses hit the news, but manufacturing losses can also affect the whole industry and can affect economic stability. Chemical engineers looked at the loss-distribution approach some time ago, they looked at Monte Carlo simulation, but LDA is still something to look at and use internally, for financial services as well as manufacturing, and there is real potential for improvement.”

The breadth of sources also allowed them to produce robust results despite the flaw in loss data collection. Individual institutions face problems with data history, quality and availability, meaning it is vital to take a wider view, he says.


Kamil Mizgier

The model allowed the researchers to measure the dependence of loss severity on internal control weaknesses. From outside, they were unable to assess firms' internal controls directly, but they used established proxies, taken by Chen from previous work in accounting theory: the size, financial health (measured as debt ratio) and reporting complexity (in terms of the number of jurisdictions and currencies the firm operated in), as well as the impact of the 2007–08 financial crisis.

Larger size and greater complexity meant more severe op risk losses. "When you're a big firm, it is hard to cover every aspect of operational management, so there is more potential for operational risk," Chen says.

Mizgier adds: "I didn't expect that internal control weaknesses would really show dependency with operational risk – some reacted more than others, but I didn't expect it just by looking at other theoretical papers. Large size is discussed widely, but here we can really see it in the data – previous work was limited by the data available."

Stress testing

The model should have many applications – both regulators and individual institutions could use it for stress testing, Embrechts suggests: "You can move from 'if' to 'what if', from value-at-risk to expected shortfall. If you can build in a structural change, we can see what the consequences are; for example, an increase in the volume of certain products."

Regulators will be able to collect industrywide data in much greater detail than outside data providers, such as SAS or ORX, he continues. Banks working at a single-institution level will be able to map their own processes and internal controls in detail, and match those weaknesses

Xian Chen

with operational risk losses directly – rather than using proxies such as size and debt ratio – and potentially discover more hidden drivers of op risk losses.

“It is a better magnifying glass for the user to look at their own weaknesses,” Embrechts says.

But the use of dynamic rather than static EVT modelling is one of the model’s most important features, Embrechts argues, allowing the tracking of actual risk exposure much more closely. The authors show this by comparing static and dynamic EVT models with actual VAR data for financial institutions. The model can also handle emerging risks better – one in particular.

“It will be very important because one emerging risk is cyber, and that will hit every industry and every part of society, not just the financial industry,” Embrechts says. “EVT gives you a way of thinking about non-normal data and that’s why it is important in this application – and in the realm of cyber risk, there will be a lot of applications. Cyber is an area where new covariates are really having a huge influence and the model we propose is very relevant. We are informed that cyber data is opening up though it’s not clear what the granularity will be.”

This makes it even more important for firms to share data on attacks and cyber losses. “We can’t say in the cyber world that big losses at one firm are their problem only – we are all in the same boat,” he warns.