BREAKING CHAINS:

HOW TECHNOLOGY LEADERSHIP SEPARATES THE PREPARED FROM THE EXPOSED

At September's Exiger: Breaking Chains, leaders explored how connected intelligence, product-level visibility and decisive leadership can turn complex supply chain risks into informed action

EXIGER

WRITTEN BY
NELL WALKER





In many of our conversations about transformation, general improvements, and change management, everything circles back to leadership. Technology leaders wear many hats, and often need to fill in gaps to ensure supply chain risks are stripped down to a minimum.

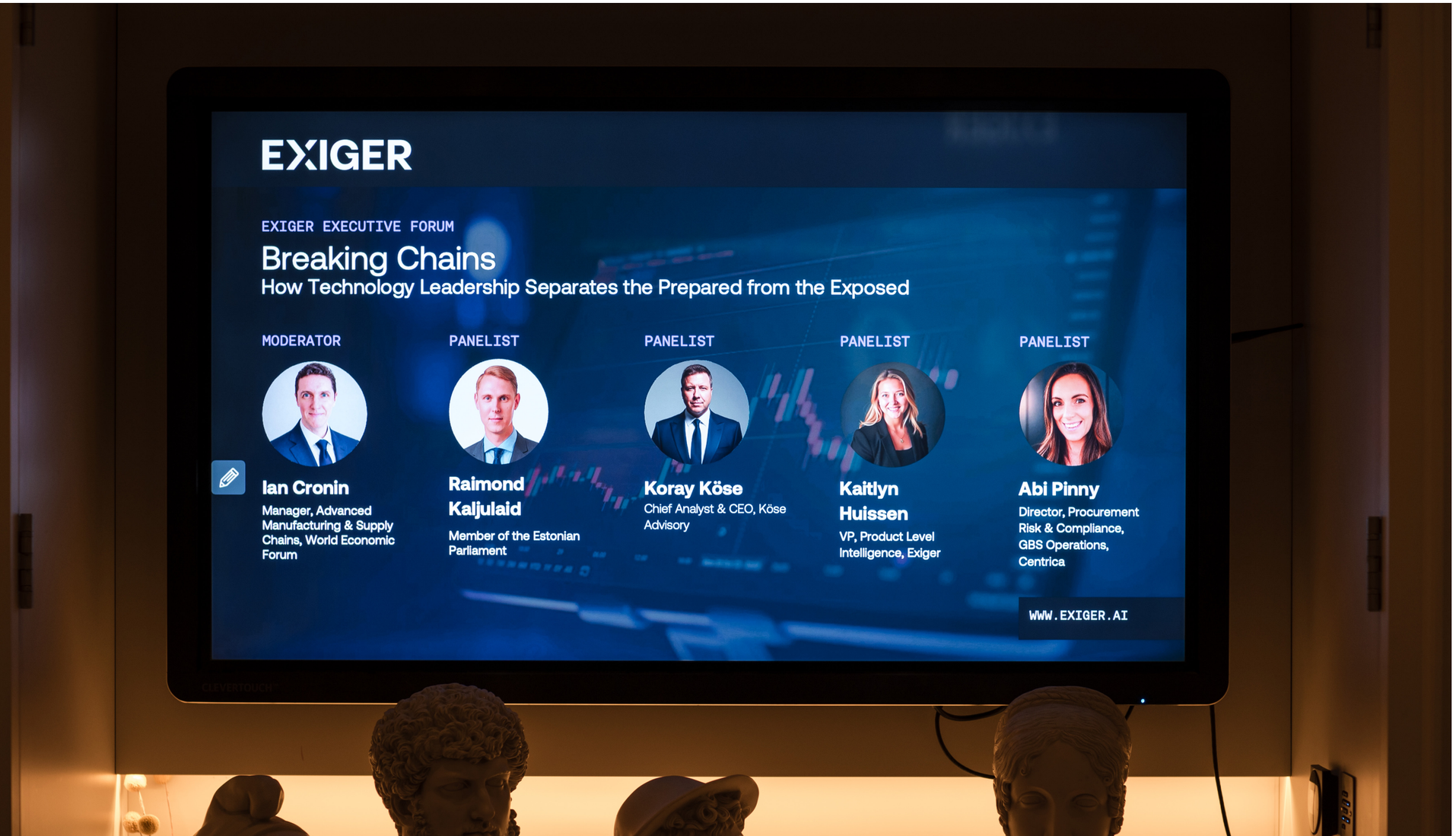
Supply chain risks now permeate every part of the chain and beyond. Across geopolitics, regulation, cybersecurity, materials, technology, and operations, risk is alive and well and navigating it is more complex than ever. Often, its first meaningful signal is financial. This is where technology leadership matters most: converting weak signals into prioritised action before the business can be put at risk.

This was the topic that shaped the most recent Exiger: Breaking Chains. On the 16th of September, supply chain experts gathered at the Great Scotland Yard Hotel in London for a panel entitled Breaking chains: How technology leadership separates the prepared from the exposed.

The panel explored how leadership, shared intelligence and technology can help organisations move from fragmented risk assessments to coordinated decisions. Ewen O'Brien, Vice President, International GTM prefaced the start of the panel by pointing out that "we're at a juncture where the norm is crisis".

"Key risk indicators are just telling you how big the exposure is, and you need to build a strong risk capacityto combat it, combined with new technology"

Koray Köse, CEO and Chief Analyst



He continued: "We're facing challenges every day that, historically, would have probably been one-in-a-hundred or one-in-a-thousand year events."

Ian Cronin, Manager, Advanced Manufacturing & Supply Chains, World Economic Forum, moderated the event. He continued from O'Brien's introduction: "What we really want to get into is the issues around supply chain management and technology. What we're seeing is that there are clear winners and losers. There are people who are using technology successfully and understanding what's happening in the risk profile, and there's people who have access to technology but aren't able to achieve the same results."

Importantly, Cronin was determined that this would not be yet another conversation about how we live in a volatile world, and we need to be agile and adaptable. "We need to get into the how," he said. "We want to get into the nitty gritty here."

At this point, Cronin introduced the panel:

- Raimond Kaljulaid, Member of the Estonian Parliament
- Koray Köse, CEO and Chief Analyst, Köse Advisory; ODI Global Advisor; World Economic Forum Expert Network Member; Senior Fellow, GlobSEC GeoTech Centre; Board Member, Slave-Free Alliance
- Kaitlyn Huissen, VP, Product Level Intelligence, Exiger
- Abi Pinny, Director, Procurement Risk & Compliance, GBS Operations, Centrica



Prepared versus exposed

Cronin kicked off the broader conversation by asking the panelists a simple question: what separates a prepared organisation from an exposed one in 2026?

“In my mind, it really is leadership,” said Kaljulaid. “When there’s a shipwreck, you don’t blame the guy in the engine room; you look at the captain and the people on the bridge.”

“Prepared organisations spot weak signals early and act decisively,” Pinny added. “Exposed organisations discover problems when customers, regulators or markets do.”

For Huissen, it’s about how a business approaches risk. “An exposed organisation is one that is still assessing risk in isolation. It’s when one compliance group is looking at risk through their own lens without a cross-functional collaboration across the organisation.”

Köse added: “A prepared organisation understands that they should probably not be hostage to the things that they are able to control and avoid those that they’re not controlling.”



Cronin then dug deeper into this with individual questions.

Compounding risk

Cronin: “From a government and geopolitical perspective, which supply chain risks have moved from temporary disruption to structural condition?”

Kaljulaid: “The way I look at these things may be from a different perspective than a business leader. As a business leader, you have – especially in a big business – the enormous responsibility of shareholders and people who work for you. But if you happen to participate in managing a country, you’ve got 44 billion euros in economic turnover that you want to grow. You’ve also got 1.3 million people to look after, some of whom are babies and elderly people. That’s a lot of responsibility, and if something drastically goes wrong, it’s a totally different thing than just a bunch of people losing money.”

The important thing, for Kaljulaid, is to be realistic. “It all sounds very negative, but there are also pockets or pillars of stability in the world. Most countries still have very sensible people in parliaments. So while international rules-based order is in a little bit of a coma right now and needs a good team of doctors, you’ve also got sources of stability.”

Cronin: “Why do conventional supplier risk models struggle when risks begin to compound?”

Köse: “Transformation has never been easy in companies, economics, or in ecosystems. They require a critical mass for everyone to understand and believe what is actually happening. For a very long time, we were fixing just one issue and then forgetting about that. And I think when we realised that there is something called compounded risk, we understood that there’s interdependency between certain decisions that we make that may be unrelated in the moment. However, in the future, they become a multiplier or magnifier of the issue. And that is something that, in a fragmented business where everybody has responsibilities and silos, just doesn’t travel.”

For Köse, supply chain has always been the outsourcing department, not the procurement department. So it’s about understanding that certain dynamics are not within your control, but there’s no going back – there’s only going forward. “If you’re trying to fix the current environment with everything that we lived in the past, you won’t actually be better.”

Cronin: “When you have these big risks you have to take action on, but they are intersecting across procurement functions,

how do you ensure that these different risk teams aren't coming up with siloed answers to the same problem?"

Pinny: "You're potentially never going to stop that happening. And I would maybe challenge the notion of having different opinions in different silos being the issue". The real benefit comes when clear ownership and accountability exists to bring those connections together and create one business decision. Businesses, organisations, leadership, they don't want five risk opinions, they want one decision.

While those multiple answers or data points are all valid and important, Pinny said, it's about the connection. Technology can now be the entry ticket to that. "You're surrounded by data. You don't even have to look for data and you're swamped by it, but actually it's about how you pull those points together and use technology to your benefit to ultimately support making those decisions."

Cronin: "What inputs do you think we need to connect to help companies understand whether they're dealing with a compound risk versus maybe an isolated incident? And how then do we see the signal within the noise using technology?"

Huissen: "When we think about risk, we're generally breaking it into different buckets. There's risks that are inherent to a specific entity. Then there are events associated with specific operating locations across the supply chain. Where is a part manufactured? Where is the material sourced? Then there is material risk, and there's systemic constraints to a raw material which you see compounded throughout the supply chain on the material risk."

When it comes to reducing that noise, it's important to understand what risk means to you and your business. "If you can't ultimately tie it back to the products that you're producing or selling, it's going to be very difficult to prioritise effort based on business impact."

Event risk versus dependency risk

Cronin then shifted the conversation to a key issue when it comes to risk, which is that many businesses focus too much energy on a single event-based risk,



"The key thing is knowing how something affects our operations or our business broadly. How critical is it? What's the size and scale of it? And how quickly will the issue come to fruition?"

Abi Pinny, Director, Procurement Risk & Compliance, GBS Operations, Centrica

rather than zooming out to look holistically at all dependency risks. When the latter is a much deeper problem, why are organisations still concentrating on those individual events?

"It's absolutely a problem," said Huissen. "It's not one specific event that is really the challenge for organisations to deal with. They're getting good at dealing with specific scenarios at this point, but anticipating the risk is more important. That's certainly the challenge."

Cronin went on to add that interpreting your own environment is part of that, "because one specific dependency or risk in a very niche area could mean something different in my organisation to yours", he said. "It's about translating that into not just what has happened with that supplier or scenario, but what does it mean to you? How critical is that?"

The discussion then turned to prioritisation: how organisations distinguish significant business exposure from the constant flow of risk alerts. Kaljulaid highlighted the importance of policy intelligence and anticipating regulatory change.

"In Estonia, we've got one of the best foreign intelligence services in the world," he said. "I sit on the oversight committee and it's one of the best. We just passed a piece

"When there's a shipwreck, you don't blame the guy in the engine room; you look at the captain and the people on the bridge"

Raimond Kaljulaid,
Member of the Estonian Parliament



of legislation that overhauls our whole crisis management system. How do we keep the country safe? How do we defend it? And the core principle is that, when something happens – a catastrophic event – we don't actually know what it's going to look like.

"How do you deal with that? You have to actually empower and enable those people and give them the authority, knowledge, and skills that allow them to act and react. With business organisations, it's kind of the same. You have to have a culture where people feel able to make decisions."

Cronin then asked the panel to consider whether procurement risk should be measured differently, including by the business consequences of an exposure rather than the presence of a risk signal alone. As part of this, he asked Pinny how to distinguish between when something should be monitored versus when a real business decision needs to be made. "The key thing is knowing how something affects our operations or our business broadly," she explained. "How critical is it? What's the size and scale of it? And how quickly will the issue come to fruition? That's probably the biggest one where technology will help us see problems before they can occur."

The panel closed by examining what distinguishes actionable intelligence from repackaged information. The test is whether technology can connect credible data to real supply chain dependencies and help teams make timely, defensible decisions, rather than simply produce another view of risk.

Prioritisation in high-risk environments

That is the distinction between being informed and being prepared. Organisations that connect product-level intelligence with business context can move beyond reacting to isolated events, prioritise the exposures that matter and act with greater confidence. As the Exiger: Breaking Chains made clear, the competitive advantage will belong not to those with the most data, but to those best equipped to turn it into decisions.

Cronin asked Huissen how a business goes from viewing business from a structural perspective of how to build supply chain solutions, to being able to see individual supplier risk and mapping out the risks of a whole enterprise. "If the foundation that those different business units or functions are looking at is relatively the same picture, then we're all looking at the same parts, we understand what those parts cost, we understand what it takes to make those parts, and who we need to source it from," she said.



"But that foundation is really viewed differently from different perspectives. An engineering person might say, 'well, this part has to be made to this specification, no compromises, irrespective of the limitations that I'm now imposing on procurement to source that from the one global source'. And so the view of part performance versus supply chain resilience is fragmented within the organisation."

At that point the question is: how do you bring that collective view into one platform? "It's by starting with the same data foundation and allowing folks to interact with that same risk lens," Huissen continued. "Then making collective decisions once we've all contributed our respective views."

Cronin then posed a bigger question: do we need to fundamentally change how we even measure procurement risk? Do we need to somehow be looking at how to evaluate the impact of these risks if they come true? And if so, how do companies go about taking on such a mammoth task?

"In a traditional sense, risk is a multiplier of whatever you do," Köse replied. "If you do something good, that good multiplies. If you do something bad, that multiplies. So there's really not just a cost equation associated to risk. What matters is the size of exposure, the risk appetite, and the manageability within the risk capacity and if it's balanced or not. So it's basically a deviation from your capability and the exposure. That's what it is at the end. If capability and exposure are balanced, you'll be better than your competitor. If not, you need to build up capability.





"Key risk indicators are just telling you how big the exposure is, and you need a strong risk capacity to combat it, combined with new technology. That's where breaking chains separates the leaders from the legacy."

And the new technology is coming. This is a key part of the conversation; yes, we're laying a lot of hope at the feet of technological advancements, but those are well on their way, if not here already. The question, Cronin posed towards the end of the panel, is: what separates a technology platform or solution that provides intelligence from a solution that's just repackaging old information? And how do we tell the difference?

"Companies are just figuring out how they're going to adopt AI," said Huissen. "People are using foundational models to ask one specific question at a time, but that only works in isolated instances. It's not extendable across the business. But if you go beyond those foundational models and look at competitors of Exiger, they're focusing their supply chain mapping efforts just on the supply chain network, providing a broad picture.

"In that respect, Exiger's approach is very different," she continued. "We take a materials-based approach to supply chain mapping. It's that full value chain or how a part is manufactured that really informs our mapping process, rather than just shipment records. That greatly increases the confidence, accuracy, and depth in our results."

The evening's conversation rounded up on this high note, with the knowledge that the technology to put an end to exposure is here, taking root. What's important is that technology leaders understand this technology, and are ready with clean and available data to make the most of it.

At a time when risk is high and there's an enormous amount of noise around how to combat that, these conversations are vital. Thank you to Exiger and the panellists for a thought-provoking discussion. We look forward to the next forum. ■

