KPMG

To manage risk with more confidence, quantify it

By Luke Nelson

Digital innovation is delivering new growth—and scores of new threats. Here's how CFOs are using technology-enhanced risk intelligence to determine which risks will have the greatest impact on their organization, so they can prioritize accordingly.

Which will have a greater impact on your organization? A malicious ransomware attack or an exposed environmental risk related to technology? For most companies, the answer, of course, is: "We won't know until it happens. (And we really hope it doesn't happen!)"

But that traditional view of risk management is undergoing a transformation of its own, with leading companies increasingly seeking a forward-looking risk intelligence approach that more accurately quantifies potential threats, allowing the business to better prioritize, fund and allocate mitigation resources.

This enhanced, technology-enabled approach to risk intelligence is being driven by the CFO and finance teams, given their view across all areas of the business and their traditional strength in risk management. For many successful businesses, the CFO has always doubled as the chief trust officer as well, a responsibility that seems to get more complex by the day as companies invest in new technologies and shared services that promise rapid growth but also introduce myriad new flavors of risk.

That's why CFOs are leaning into the concept of technology-enabled risk intelligence, which uses advanced data, analytics and automation to more precisely model and quantify potential threats. This generally ensures that the rest of the company has the confidence to focus on productive growth, rather than being slowed down by "what if" concerns about self-inflicted damage

Rethinking risk mitigation

Technology is a powerful engine of business growth, with investments in digital innovation, advanced data and analytics, automation and artificial intelligence already delivering dazzling new profits and cost efficiencies. The irony is that those same innovations have also dramatically expanded the risk landscape, with everything from increased customer data exposure to a growing reliance on third-party cloud-based service partners.

Astute CFOs have turned this seeming paradox to their advantage. Enter the concept of technology-enabled risk intelligence, which uses many of those same technology methodologies to quantify, model and mitigate the increasingly exotic risk pool by level-setting each risk on the single attribute they all share—i.e., measurable financial impact.

Traditional risk mitigation has been more art than science, focusing on the odds of an event occurring, but then relying on executive instinct to prioritize the related allocation of risk mitigation efforts and investment. With technology-enabled risk intelligence, CFOs are able to set a dollar value on the financial impact of various identifiable threats, risks and vulnerabilities, which establishes an accurate, side-by-side comparison model that precisely informs how they invest and allocate mitigation resources.

This enhanced approach to risk intelligence can more accurately quantify risk dollar impact and then integrate that information into an advanced modeling framework, powered by its own set of advanced technology tools, including artificial intelligence, automation and natural language processing.

The result: increased overall confidence across the company on activities that serve business continuity and resilience. And beyond just ensuring the right allocation of mitigation investment dollars and resources, the technology risk intelligence approach also provides essential context for how decision makers manage and update strategies going forward.

Making it happen

To get started on the path toward enhanced technology risk intelligence, the finance team will first need to evaluate three foundational areas:

- **Inventory:** Take careful inventory of the current technology landscape to ensure there is a consistent enterprise technology taxonomy and framework to build from as well as a clear view of all assets and any related controls.
- **Processes:** Build a comprehensive understanding of incident management processes to capture current data loss concerns so that new and improved financial impact models can be developed.
- **Requirements:** Establish detailed requirements for capturing, analyzing and reporting risks, and be sure to incorporate feedback from the required cross-functional teams.

With that current-state view in place, the team can then move to establishing an even more robust, technology-enabled risk management platform. CFOs can now look to the third-party marketplace for increasingly powerful, sophisticated technology risk assessment solutions. The best of them combine data filters, advanced analytics and risk domain knowledge, bundled as prebuilt offerings that always assume some degree of custom configuration to a company's specific requirements.

If the general objectives are increased risk visibility and actionable insight, then CFOs should look for features such as:

- **Data engines** that ingest historical financial data, publicly reported information, and all relevant risk and control metrics, to identify patterns of risk correlation and quantify those with greatest financial impact.
- **Investment planning**, based on risk modeling that simulates the impact of funding specific risk and control, tailored to the company's risk appetite.
- **Continuous assessment**, delivered by dashboard reporting to the client's business leads, to assess the financial impact of technology threats on an ongoing basis, down to the control and asset business.

CFOs who find solutions with these attributes will do well to apply an extra layer of scrutiny, in with two open-ended questions: How do the discrete features of a technology risk intelligence solution interact with each other to deliver additional, synergistic value? And how strong is the commitment of the provider to continuous improvement, as demonstrated by steady investment in data, analytics, technology and risk-domain frameworks? Not all third-party, technology-enabled risk intelligence solutions—or solution providers—are equal.

Every CFO knows that the force-multiplying advantages of digital enablement have come with an associated, though not always direct, increase in risk complexity. In this case, the problem contains the seeds of the answer: Risk solution intelligence, based on digital technology, will allow CFOs to maintain and fortify their role as the company's overall security protector in a fast-changing risk landscape.

Find more related CFO insights at visit.kpmg.us/CFOperspectives.

Contact us

Luke Nelson
Managing Director,
Technology Risk Management
+1 515 697 1214