Deloitte.

The language for translating government cyber risks into outcomes

While each department or agency may have a unique assessment of the impact of different risks, assessing those risks against a risk quantification model allows them to communicate in the same language.

In 2020, more than 18,000 organizations around the world installed a software update from their provider, SolarWinds—not knowing it was contaminated with malicious code. The massive cyber vulnerability—which impacted public sector organizations, as well as private businesses—proved to be a stark wake-up call for all involved and shone an unflattering spotlight on the gaps in cybersecurity across government agencies.

In response, many governments are now taking action and exploring ways to better assess cyber risk, both internally and externally. The US Congress, for instance, recently required all US government organizations and agencies to adopt a single formula to quantify cyber risk by 2024. The move, which mirrors actions taken by the European Union, is intended to encourage greater transparency around how risk is calculated. By implementing a common language, the US Congress hopes government and agency leaders will have better access to the actionable information they need to measure their process and departmental risks, and protect their society, citizens and economy.

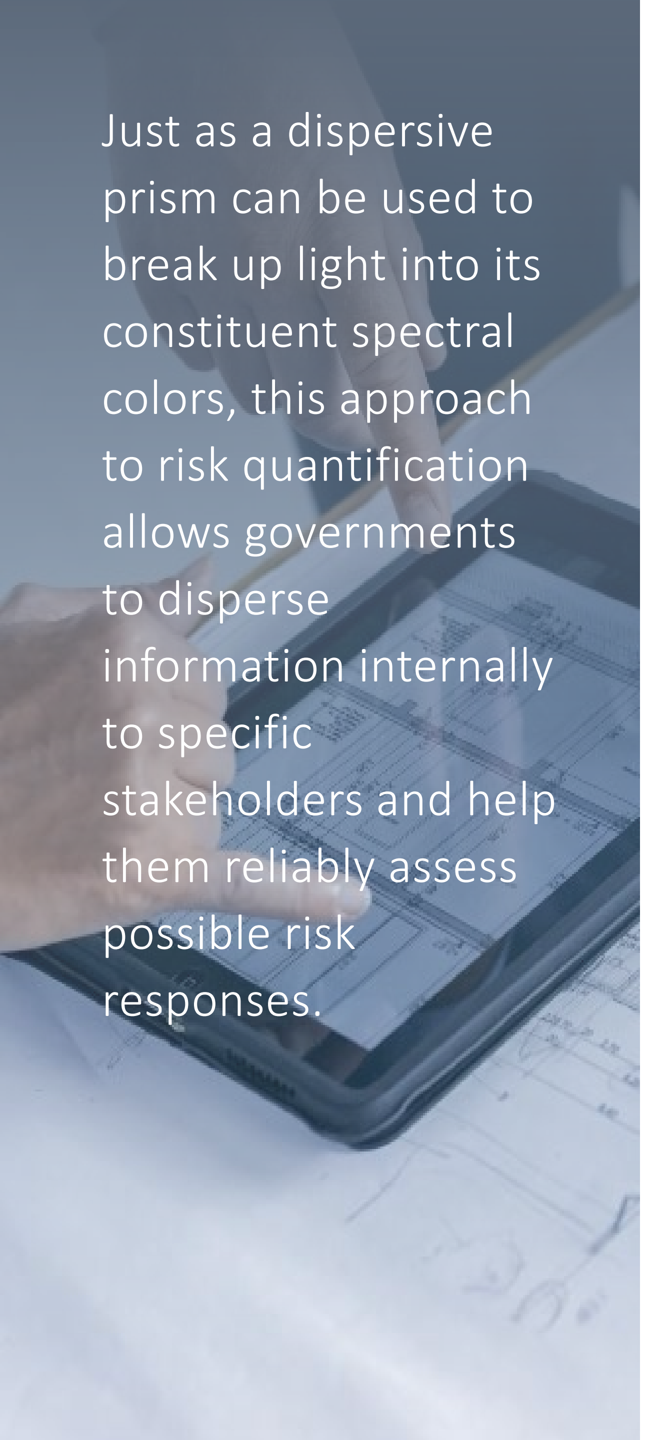
Adopting this common formula will be no easy feat. Every level of government—and every governmental agency—faces unique cyber risk environments. As a result, they all have different methods of measuring risk, making it difficult to prioritize cybersecurity investments. Even within a specific agency, there can be a disconnect in how risk is assessed. For instance, there may be a technical security gap in how a government revenue authority issues its annual refunds. While a CISO may be able to identify this issue, if they can't convey it in a way that connects the risk to the mission of issuing a refund, agency leaders may not prioritize it.

To overcome this hurdle, governments need to take a unifying approach to aggregating data and make information more consumable and sharable across branches and agencies.

Creating a common language

Taking action on cyber risk involves making sure leaders understand how the associated data—and emerging risk insights—impact their role, mandates, competing priorities and evolving relationships.

This is where *information theory* proves to be invaluable. This field of scientific study allows leaders to more effectively quantify, store and communicate digital information through foundational rulesets and prioritization frameworks.



Just as a dispersive prism can be used to break up light into its constituent spectral colors, this approach to risk quantification allows governments to disperse information internally to specific stakeholders and help them reliably assess possible risk responses.

Essentially, when building a customized risk quantification model with information theory as its backbone, you can couple information from a standard or regulation—such as the NIST, ISO, COBIT or GDPR—with scientifically-informed measures, so there's a common language for controls. From there, you use the power of machine learning to map the organizational imperatives and risks, and leverage information theory to pre-curate existing data. By the end, you have a relative risk evaluation system (which communicates more effectively than a risk scoring system alone)—or a consistent way to assess risk across the government. This allows machine learning recommendation engines to suggest forums for different agency leaders to engage with, or identify groups most likely to mitigate a specific type of risk.

With this foundation in place, each agency or department can build an individualized risk framework to reflect their unique risk environment. This sub-framework can help your department prioritize its unique cybersecurity efforts while aligning to consistent governmental standards. In short, while each department or agency may have a unique assessment of the impact of different risks, they're assessing those risks against a risk quantification model that allows them to communicate in the same language.

From information into action

Just as a dispersive prism can be used to break up light into its constituent spectral colors, this approach to risk quantification allows governments to disperse information internally to specific stakeholders and help them reliably assess possible risk responses.

For instance, once leaders clearly understand the cyber risks facing their departments—and it's conveyed to them in a business-friendly, non-technical manner—they may be more inclined to introduce security early in an app-building process rather than at the end.

In the case of the aforementioned government benefits authority issuing annual refunds, for example, this would allow the CISO to build datasets around the security coding processes for the applications most relevant to the function. Using the common framework, they could easily define what different types of vulnerabilities mean to different elements of the process—such as receiving or issuing payments—and assign each element a risk score. Leaders, then, could more effectively assess which risks need to be addressed to roll the app out with confidence.

A government health organization looking to enhance its security operations and better assess its security risks could be another example. By building detailed templates around multiple layers of the stack (e.g., ranging from third party libraries to middleware) and different asset types (e.g., medical devices and health care facilities), the organization could more effectively curate its existing data and apply it to fit its unique mission.

While the organization wouldn't be able to predict what risks would arise from week to week, this approach would nevertheless provide it with the ability to dynamically connect the risk story to the mission. For instance, by speaking to the owner of the health care facility, the organization could better understand the security risks facing patient services. At the same time, the organization would also be aware of the research leader's priorities—and devise a solution that could simultaneously help them protect their medical research objectives.

These are just a few examples of how a common cyber framework and language can help with application security, but there are many others. For instance, this cyber approach can also help departments:

- Assess the risk profile of a product earlier in the process and compare it against a baseline level of controls
- Solve for inconsistency of controls across product development
- Determine where money needs to be committed across the development cycle and when to invite the security function to the table
- Break down silos and provide visibility and transparency across the full product life cycle
- Automate workflows to other security functions (allowing them to understand security issues before an app hits production)
- Highlight potential areas of vulnerability through threat modeling

Paving a path forward

There's no question we've entered a new era of cybersecurity—and cyber risk quantification is an emerging practice. That said, with the right templates and guidance, it's possible to apply this model successfully across multiple jurisdictions and departments.

Authors and contacts

Srini Subramanian| **Global GPS Leader**
ssubramanian@deloitte.com

Andrea Rigoni | **Global Cyber GPS Leader**
arigoni@deloitte.it

Mark Nace |US Cyber GPS Leader
mnace@deloitte.com

John Gelinne | **US Cyber Risk Quantification Leader**
jgelinne@deloitte.com

Kelly Miller Smith | **US GPS Cyber Risk Quantification Leader**
kellysmith@deloitte.com

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see http://www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the "Deloitte organization") serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 330,000 people make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.