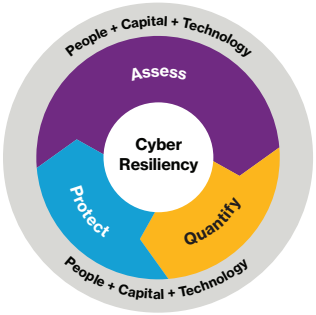


Decode risk.

Find your cyber "North Star": Use enterprise risk management to prioritize cybersecurity investment

by Tom Finan, Willis Towers Watson

Many questions surface when formulating a cyber risk strategy, but there is one that gets right to the heart of the matter: What cyber risks pose the greatest threat to the success of our business? In other words, what cyber risks should we care about most? The answer, and who provides it, can serve as a powerful cyber "North Star" that will promote highly successful cybersecurity outcomes.

Enterprise risk management's role in cyber strategy

Every new cyber incident seems to up the ante when it comes to making the right cybersecurity "bets" to avoid the breaches, business interruption, fines, and profound reputational damage that a cyber incident can cause. Fortunately, many excellent authorities exist that can help guide the development of a strong cyber risk management strategy. For instance, cybersecurity vendors are constantly creating new and better solutions to thwart cybercriminals.

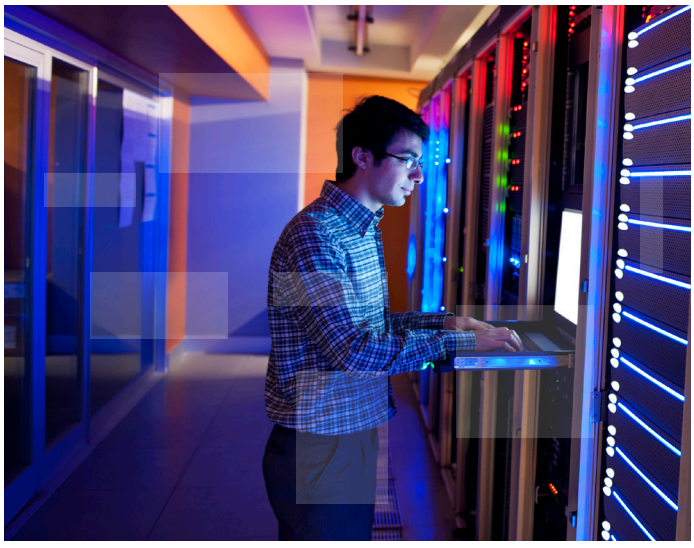
The stakes are high, and executives are under a lot of pressure to get their cyber programs right. But there's good news. Enterprise risk management (ERM) can significantly increase the likelihood that organizations will navigate the right course and effectively address their unique cyber risks.

ERM has been around for a long time, but business leaders only recently have begun to use its principles to treat cyber risk like any other important business risk. Why? Because executives have increasingly realized that the central goal of a truly effective cyber risk management program is to support the successful accomplishment of an organization's key business goals and objectives. A cross-functional approach that engages six key leaders across the enterprise offers that assurance.

Thought-provoking questions to inform your cyber strategy

As organizations develop their cyber risk programs, consider these important questions:

- How are we implementing the National Institute of Standards and Technology framework?
- What does ISO 27001 mean for our cyber risk management priorities?
- Should we buy more encryption or implement two-factor authentication?
- Are we paying attention to the human element of cyber risk?
- What about the General Data Protection Regulation (GDPR)?



Willis Towers Watson

Roles and responsibilities

Six key leaders have a unique understanding of their organization's mission-critical functions that must go off without a hitch, the highly sensitive data that must be prioritized for protection and the quantum of financial and reputational harm that a serious cyber failure could cause. Each also knows what cyber risks keep them up at night, those that can be tolerated and which intolerable risks should be prioritized for action. These leaders are:

Chief Information Security Officers (CISOs). CISOs develop and implement their organizations' information security programs. They focus on identifying and mitigating cyber risks to the business and must anticipate new threats and work to prevent their occurrence. CISOs may conduct employee cybersecurity training, enforce compliance with security practices, and partner with Chief Information Officers (CIO) to purchase necessary cybersecurity products and services.

- **Chief Information Officers (CIOs).** CIOs meet their organizations' information technology (IT) needs, by ensuring that the IT systems in place create value by supporting the accomplishment of key business goals and objectives. They lead and otherwise collaborate with CISOs and others on a wide range of information security, customer experience, and data initiatives to reduce risk and grow revenue.
- **Chief Risk Officers (CROs).** CROs have primary responsibility for developing their organizations' risk frameworks and associated policies, managing their risk appetites, and advising their boards and C-suites about all manner of business risk (including cyber). CROs address those risks at the enterprise level with a strategic focus on ensuring the achievement of key business goals and objectives. CROs often lead their organizations' insurance negotiations and purchase decisions.
- **Chief Human Resources Officers (CHROs).** CHROs play a critical cybersecurity role when protecting highly sensitive personal information of past, current, and future employees. They implement strategies to recruit and retain key cybersecurity personnel and collaborate actively with CISOs and others to protect their organizations from insider threats. CHROs may lead, or work with CISOs, to deploy cybersecurity training and awareness programs for employees.
- **Chief Financial Officers (CFOs).** CFOs focus on the results of their organizations' cybersecurity expenditures: Do they provide a positive return on investment measured by fewer and/or less severe cyber incidents? Do cyber risks holistically consider both technical and human risks? Are emerging risks on everyone's radar? They're also responsible for ensuring the security of sensitive financial information and compliance with applicable laws and regulations.
- **General Counsels (GCs).** GCs concern themselves with the legal implications of failing to address their organizations' cyber risks properly. Compliance with new legal regimes like the General Data Protection Regulation, the New York Department of Financial Services Cybersecurity Regulation, and state data breach notification laws requires their constant oversight of cybersecurity programs and practices. GCs also focus on privacy issues and minimizing liabilities associated with their organizations' cyber risk profiles.

Going down the right path

A good start to truly understand an organization's cybersecurity maturity is to reach out to these six key leaders. Collectively, their responses will quickly clarify an organization's cybersecurity strengths and weaknesses, and what fixes, if prioritized, would likely provide the greatest return on cybersecurity investment. Surveys, individual interviews and a final consensus discussion will help senior management to fully comprehend what work needs to be done. The information gathering process could query these six leaders on issues such as the enterprise's ability to identify key people, process, data, and technology assets, and the ability to effectively respond and recover from an incident once it's discovered. Ultimately, this information will serve as a guide to decision making about worthwhile technical and human capital investments — a veritable cyber North Star.

Key leader discussions

Survey responses are likely to reveal significant divergence of opinion on an organization's cyber risks, making it important to interview the six key leaders separately. This presents an opportunity to share survey results and potential solutions to identified shortcomings, zero in and discuss areas of disagreement and inquire about particular risks that raise concerns.

There's good reason to take this holistic approach. A CHRO, for example, may have particular employee data at the top of their "need to protect" list that is nowhere near being on the CIO's or CISO's radar. The CFO may emphasize the security of a particular payment system as a key asset upon which the organization's very existence depends — a priority not known to the CRO. And the GC may be aware of a new privacy requirement and associated regulatory penalties that must change how all these colleagues do business.

None of these insights will be accessible without a targeted investment of time in one-on-one key leader interviews. Senior management should designate a person or team to conduct both the initial survey and these follow-up conversations and then synthesize what's discovered. The synthesis will help set the agenda for a group discussion during which an organization's cyber North Star will emerge clearly and guide cybersecurity activity and investment decisions.

The power of consensus

A productive group discussion, gives each of the six key leaders the floor to share views expressed during their individual interviews, to react to the collective survey results, and, perhaps most importantly, to listen to the perspectives of others. Often, this kind of exchange is the first time these leaders will have focused together on cyber risk for any sustained period of time. Senior management should take advantage of the opportunity to facilitate a full and fair discussion.

This is where an organization's cyber North Star – informed consensus – shines. An exchange of ideas encourages collaboration informed by a clear understanding of the full spectrum of cyber risks to the business. Consensus better prepares these cyber leaders to make critical decisions about which cyber risks to prioritize and what corresponding courses of action will provide the greatest security return. But that's not all. The collective buy-in that this informed consensus promotes will ease the implementation of chosen, near-term risk management strategies. It will also help establish the foundations of a familiar forum that will enable productive future discussions about emerging cyber risks.

Find your cyber North Star

The cyber North Star is different for every organization. Finding yours – and following it – will ensure more effective, business-supporting allocations of resources, facilitate the implementation of impactful controls, and promote continuous conversation among your key leaders that will bolster your cybersecurity for years to come.

Contact

Tom Finan
Director, Cyber Risk Solutions, North America
+1 703 258 8469
thomas.finan@willistowerswatson.com

willistowerswatson.com/social-media