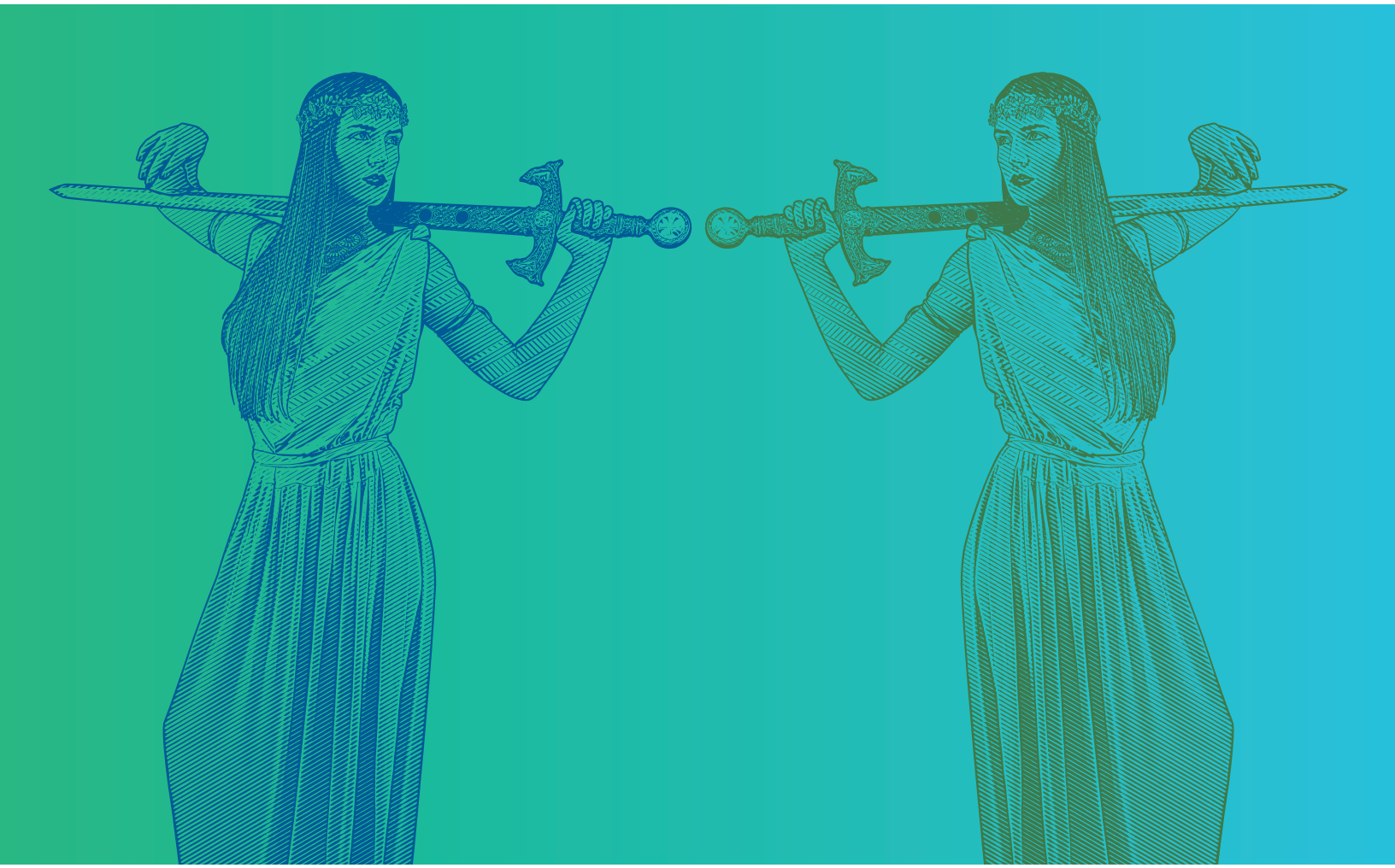
Cybersecurity and the risk function

Are your information technology, cybersecurity, and risk professionals working together as a championship team to neutralize cyberthreats and protect business value?

Oliver Bevan, Jim Boehm, Merlina Manocaran, and Rolf Riemenschnitter



NOVEMBER 2018 • RISK PRACTICE

Most CEOs of large organizations are convinced of the existential dimensions of cyberrisk. The most savvy have begun to approach cybersecurity with an enterprise-wide perspective, involving the teams of the chief information security officer (CISO), the chief information officer (CIO), and the chief risk officer (CRO), as well as the business units. A true partnership between these teams is the optimal approach, having emerged from a recognition that no single leader or team can gain the complete perspective needed to be effective in the cyberdomain. No one group within a company could manage the number and types of internal and external threats, the complex technological landscape, and the many actions needed to address vulnerabilities associated with people and technology. They rather need to work together.

The status quo: CISO-only control

A collaborative, enterprise-wide approach has not yet been widely adopted, however. For many companies, de facto responsibility for cybersecurity has devolved almost exclusively on the chief information security officer. The CISO may work with teams led by the CRO and the CIO, but collaboration usually occurs on an ad-hoc basis rather than within a coordinated strategy. As such, the risk function will not participate to the extent needed to embed business-risk awareness in a company's cybersecurity posture and planning nor to align the strategy with the company's business-risk appetite. Without a risk-based focus on cybersecurity, companies often overlook the true drivers of risk, an error that can magnify a crisis and lead to unnecessarily large business losses. One of the challenges to collaboration has been the technical nature of the cybersecurity environment, an abiding condition that must be addressed when organizations embed the risk function and risk thinking in cybersecurity strategy. Risk organizations can find it difficult to contribute meaningfully to tech-based discussions. Conversely, cybersecurity teams can be reluctant to add risk processes—such as risk and control self-assessments—to their agendas, overfull as they are with complex technical tasks. A further complication is the tendency of executives and board members to rely exclusively on the CISO and the CISO team whenever they face a cybersecurity issue. This usually adds pressure on an already overtaxed team while reinforcing the notion that the CISO has the only point of view on the topic.

The urgency of a risk lens

In theory, the risk function is charged with managing all operational risk across the organization, but under the CISO-centered arrangement for cybersecurity, the risk function is often sidelined in the area of cyberrisk. The absence of the essential risk perspective can skew the cybersecurity stance irrationally: either toward issues of the most immediate concern to senior leaders or toward the security scare du jour. Such biases potentially magnify the danger of the actual vulnerabilities being ignored. Risk oversight of cybersecurity practices can ensure that the strategy protects the most valuable assets, where a breach would pose the greatest potential business damage, whether in terms of reputation, regulatory intervention, or the bottom line. A simultaneous benefit is that this risk lens helps to control costs. The inevitability and proliferation of cyberattacks make mitigation of every risk financially impossible. Companies must therefore review all risks across the organization, locating and mitigating the most significant ones, applying protection, detection, and response interventions in a prioritized way.

Fulfilling this obvious requirement, to prioritize the most important risks to the enterprise, is practically difficult within the CISO-centered approach. The task can be especially hard for CISOs and other security professionals whose training and experience has centered on designing and implementing strong security protections, or running a security-operations workflow. Risk management—the identification, quantitative evaluation, and prioritization of risks—is outside their main focus. Of course, these are exactly the purposes of the risk organization. In nearly every other area of the business, the risk group is constantly identifying, evaluating, and remediating risks. Risk should be doing this for cyberrisk as well. The question is, how best to integrate risk into the cybersecurity environment?

Barriers to CISO–Risk collaboration

While organizational models for handling cyberrisk vary across institutions, several shortcomings are commonly observed. The most basic has been a lack of clarity in how the lines-of-defense concept should be applied. This concept, as developed by financial institutions to manage risk in the regulatory environment, clearly delineates three lines—business and operations managers, risk and compliance functions, and internal auditors.

For cyberrisk, the lines-of-defense concept can be seen in the roles of the cybersecurity function as the first line of defense and the risk function as the second. That is, the cybersecurity function, usually as an integral part of IT, initiates the risk-mitigating interventions that protect against, detect, and respond to threats generated in business and IT operations. As the second line of defense, the risk function works with the first line to identify and prioritize cyberrisks.

In practice, some blurring of these boundaries occurs (and a healthy exchange of perspectives is recommended), as organizations work collectively across the lines to identify risks and mitigate vulnerabilities. The "blurring" does not, however, diminish the importance of the challenge responsibilities of the second line of defense. It rather provides the second line with the opportunity to challenge the first line more often in open dialogue. As will be seen, this relationship benefits both the first and second lines. The first line becomes more aware of how cyberrisk fits into enterprise risk management and better prepared for arising risk challenges once interventions are under way. The second line, meanwhile, becomes more familiar with the capabilities and plans of the first line.

The lines-of-defense concept can be seen in the roles of the cybersecurity function as the first line of defense and the risk function as the second.

In CISO-centered approaches to cybersecurity, the CISO team can be responsible for all roles across the lines of defense. The team might identify the cyberrisks, decide on the investments in mitigation, design the technical and nontechnical security controls, manage the resources needed to implement controls and operational initiatives, and determine how risk-reduction efforts should be measured and reported. The same function (and sometimes the same person) will thus perform or direct all risk-identifying and risk-reducing activities and then certify whether the activities are working. (Not surprisingly, under such an arrangement, the reporting usually shows that progress has been good.)

At some companies using a CISO-led approach, the risk function theoretically plays an oversight role as the second line of defense. Yet meaningful insight into cybersecurity activities cannot be obtained without deeper engagement. Often the CRO will have no clear mandate for this kind of involvement and will find it organizationally difficult to challenge CISO-controlled activities. Other obstacles include a lack of cybersecurity skills within the risk function and an insufficient view on the unit of risk (the information asset) and the corresponding value at stake. In short, if the risk function is not integral to risk assessment and remediation in the cybersecurity space, it will be unable to play a meaningful challenger role. Instead, for reports and additional information, CRO and team will be dependent on voluntary cooperation, often initiated after events—too late, that is, to do much good.

Organizational friction

As when the CISO controls all aspects of the cybersecurity strategy, issues can also arise when cyberrisk responsibilities are formally divided among two or more teams. If the operating model for the division of responsibilities is inadequate or has not been fully implemented, silos can develop, generating organizational friction.

At one company, the CRO and experts within the risk organization crafted all cyberrisk policies in accordance with the company's risk appetite and then assessed adherence by the CISO, CIO, and business units. The CRO also informed executives and the board of the top risks, advising on a course of action and reporting on progress. The CISO was responsible for designing the technical and manual controls, and for executing risk-mitigating initiatives. Detailed implementation was the responsibility of the CIO. Despite the clear delineation of roles, significant organizational friction arose.

At this company, the risk function was rightly trying to take on a more integrated role, based on its knowledge of adjacent relevant risks, including fraud and vendor risk. Yet because risk and security were so heavily siloed, the risk function proceeded without much collaboration. The CISO and CIO teams were given little opportunity to provide input before being presented with finished requirements. Unsurprisingly, they reacted negatively, tending to regard the policies and targets as unreasonable, unattainable, and therefore irrelevant. At this point, the chances of gaining the cooperation needed to improve outcomes were much reduced. And things regressed from there, as the CISO and CIO teams mostly ignored the risk function. Eventually the executive team supported the CISO and the risk function was deprived of its deeper role in cybersecurity.

Friction between different parts of an organization drives up costs, wastes resources, and impairs alignment—in this case, alignment around an enterprise-wide strategy to reduce cyberrisk. When this happens, a kind of risk blindness can afflict everyone involved. The situation will eventually become apparent to top management and the board, after they receive piecemeal reports on cyberrisk outcomes from different groups in a variety of formats and frequencies. These leaders must be forgiven if they wonder whether the right hand knows what the left hand is doing.

A strategic security partnership

Many CISOs and CIOs would like to integrate their vantage points more deeply into the enterprise risk process, and the risk function can and should be better involved in cybersecurity. However, best practices for achieving risk's optimal role in identifying, prioritizing, and managing cyberrisk have only begun to emerge. Many companies have struggled to define and distinguish the duties of all relevant parties clearly and logically, so that they can interact effectively and in the right sequence to actually reduce risk. But some companies are finding a better way.

We see emerging best practice in an approach we call a "strategic security partnership." Motivated by an explicit mandate from executive leadership, the approach involves the full commitment and cooperation of the CISO, CIO, and CRO teams in the cybersecurity space. To implement the approach, an integrated operating model needs to be carefully plotted and tested, starting with the key processes around which an organization and culture are designed. What follows is a sketch of this method as successfully implemented by one large corporation.

1. The role of the chief risk officer and the risk team

- In partnership with the CISO and the security specialists, the risk team forms an early view of the cyberrisks across the enterprise, including such adjacent risks as fraud and vendor risk. This early challenge of potential first-line interventions helps foster the collaboration needed for a more effective and efficient process to prioritize risks for remediation.

- The CRO helps the CISO and the CIO design the principles of cyberinvestment for the company.

- The risk team works with the CISO and the CIO to develop and present the overall portfolio of initiatives to executive management.

- Risk independently monitors the progress and status of initiatives as well as the outcomes of cyberinvestments and mitigation. The team also collaborates with the CISO and CIO to work out reasonable mitigations and timelines when agreed-upon guidelines are violated.

2. The role of the chief information security officer

- With the guidance of the chief risk officer, the CISO and team translate the cyberrisk recommendations into technical and nontechnical initiatives. The CISO vets and aligns them with the CIO team, since initiative design, architecture, and implementation will require CIO resources. The teams of the CISO, CIO, and CRO jointly approve the program of work. The CISO team works with the CIO team to design the solutions to fulfill each initiative.

- Together with the CRO, the CISO aligns the format, content, and cadence of cyberrisk reporting, so that cyberrisk is reported with all other risks. The CISO and the CIO implement reporting initiatives and jointly report on progress and status to the CRO, who then reports to the executive leadership and the board.

- Either alone or together with the CIO, the CISO directs a security operations center (SOC). In a successful case, the operations center is jointly run, with the CIO team focusing on the operational workflow and the CISO team providing security-specific support, including threat intelligence, forensics, and red team–blue team exercise planning. Even if the CISO team has full control of the SOC, however, it will need to work closely with the CIO teams running IT operations such as network or production monitoring.

3. The role of the chief information officer

- As indicated in the foregoing discussion of the CRO and CISO roles, the CIO team has an equal stake in addressing cyberrisk throughout the processes. Their equality is absolutely essential, since CIO and team are primarily responsible for implementation and will have to balance security-driven demands for their capacity with their other IT "run" and "change" requirements.

The advantages of a strategic security partnership

The advantages of a strategic security partnership will usually outweigh the challenges of adopting it. First, this approach ensures that risk-based thinking is embedded in the CISO's program, breaking down functional silos and laying the foundation for eliminating the organizational friction that characterizes CISO-only control. With top-management leadership, most institutions can implement a strategic security partnership immediately. For organizations that already have risk, CISO, and CIO teams, the approach requires no new hiring and no significant change in responsibilities. (For the sets of actions the transition will require, see the sidebar, "Moving risk from status-quo cybersecurity approaches to a strategic security partnership.")

A strategic security partnership establishes the needed relationships and perspectives up front. This advantage can be of great importance in the event of a cybersecurity incident: the CISO and the CIO will already have a risk-informed view and understand the risk to the business. The CRO, meanwhile, will understand what the CISO and the CIO can and cannot do. Under a strategic security partnership, all three leaders know how to work with one another and how to bring in the business units as needed. Crucially, they also understand the importance of clear, trustworthy internal and external communications during an incident, as the CISO and CIO teams get down to the business of containment, eradication, and remediation.

Fixing leaks . . . together

Given the number of functions involved and the complexity of the tasks, the processes of identifying and prioritizing risks, aligning the program, and agreeing upon and implementing initiatives can be time-consuming. An essential purpose of the model is to ensure that the CRO and the risk group understand cyberrisk at the level of each information asset and the relative business value entailed. Without this essential insight, risk prioritization cannot proceed. The principals involved can work to improve coordination, but they must allow enough time for these crucial processes to be completed properly, since the potential effectiveness of the outcomes will be much greater.

Fine tuning will probably be needed to sharpen the definition of roles, responsibilities, and decision rights. No one should be surprised if confusion arises about who owns what task, but proper planning can reduce the confusion. Exercises using "RACI" process diagrams are the best remedy. The acronym stands for "responsible, accountable, consulted, informed," and the diagrams are used to identify roles and responsibilities during an organizational change. "Water through the pipes" (WTTP) exercises are used for testing: process flows are initiated and where "leaks" in the clarity of the organizational plumbing are detected, the RACI-based diagram is repaired with agreed-upon changes. The diagrams are validated by the teams and aggregated with corresponding workflows into the comprehensive operating model. This additional exercise should completely remove any residual organizational friction. It sharpens roles and rights while laying the groundwork for good working relationships, as all concerned spend time around the table jointly solving problems to arrive at the optimal solution for all stakeholders.

Insights on model performance

For the model to perform optimally, decision makers should be few in number. They should be trusted members of each organization. They will

An essential purpose of the model is to ensure that the CRO and the risk group understand cyberrisk at the level of each information asset and the relative business value entailed.

Moving risk from status-quo cybersecurity approaches to a strategic security partnership

The strategic security partnership described in this article is a new cybersecurity approach, not yet common among large companies today. The status quo environment is more defined by two models, in which the role of risk is either to act mainly as a challenger or mainly as a policy setter and adherence checker. In the former model, risk is less involved in cybersecurity: tech-savvy risk-team members take the initiative to ask the teams of the chief information security officer (CISO) and the chief information officer (CIO) for answers to specific questions or to supply risk with more detailed reports. In the latter model, risk sets the cyberrisk policies to which the CISO and CIO teams are expected to adhere. As policy setter and adherence checker, risk also controls reporting to the executive leadership and board.

In our view, each of these widely deployed approaches is fundamentally inferior to the strategic security partnership. Depending on which approach prevails in an organization, different sets of actions will be needed to migrate risk to the superior model.

1. Risk as challenger

These are the status-quo roles:

- The CISO, sometimes in collaboration with the CIO, identifies and prioritizes cyberrisk, sets the agenda for cyberinvestments, and determines policy limits for IT and business behavior. The CISO is also responsible for the design and architecture of both technical and nontechnical security controls, and performs other first-line functions, such as security operations. The CISO may also own the resources necessary to implement control and operational initiatives, though more often these will come from the CIO organization. Importantly, the CISO is also in charge of all measurement and reporting of risk reduction to the executive leadership and the board.

- The CIO sometimes partners with the CISO for the more technical design aspects of the program. While the CISO may direct implementation, the CIO is usually responsible for the actual implementation work, sometimes reporting progress to the CISO, sometimes to the executive leadership directly. In some cases, the CIO may direct security operations, with the CISO acting as a "1.5" or second line of defense.

- The role of the risk team in the challenger model is to ask the right questions of the CISO or sometimes ask for more detailed reports. Effectiveness depends heavily on the timing of risk's involvement, the stature of the risk team, and its level of technical knowledge. Without the right combination of these elements, risk may find it difficult to understand what is going on and can easily be sidelined.

These actions are needed to migrate from the challenger model to a strategic security partnership:

- The risk team will need to acquire additional skills and knowledge to engage the CISO and CIO teams on cybersecurity in a meaningful way.

- To provide a business-risk perspective on what is desirable and reasonable, risk needs to be present at meetings on policy planning, architecture, and the implementation of nontechnical controls. The role of risk will include helping the CISO and CIO teams understand how their concerns connect to business risk. Together, the three teams will then be able to shape the year's cyberrisk agenda on an enterprise-wide basis.

- CISO and the chief risk officer (CRO) will together create a truly risk-reducing performance-management plan. The measurement and reporting activities performed by the CISO team need to be aligned with business objectives, following the model of the way risk works with business-unit leaders. Together the CISO and CRO teams will determine reasonable and achievable targets, bringing in the CIO team for the program-delivery plan. Metrics based on relevant insights and data sources can then be developed.

2. Risk as policy setter and adherence checker

These are the status-quo roles:

- Risk determines the cyberrisk policies that the CISO, the CIO, and business units are expected to follow and then assesses adherence to them. Ideally, policies are developed by cybersavvy members of the CRO team and implemented according to the enterprise-wide risk appetite, though the reality is often different. Risk also owns all reporting, including reporting on the top cyberrisks, on the policies to address them, the adherence levels of the CISO and CIO, and the status of the initiatives being implemented to address the top risks. While this reporting should be aligned with reports produced by the teams of the CISO and CIO, it is too often produced in a vacuum.

- The CISO receives the risk appetite and policies from risk and then designs (and may also build) technical and non-technical controls, sometimes in partnership with the CIO. The CISO or the CIO may direct security operations, according to service-level agreements (SLAs) and tolerance levels set by risk. The CISO is responsible for executing the program of initiatives, though the CIO's organization usually does the hands-on work. The CISO reports to risk and to the leadership and board on the progress and status of initiatives. Depending on the level of organizational friction, either the CISO or the CIO may remediate areas raised by risk.

These actions are needed to migrate from this model, with its divided and sometimes conflicting authority, to a strategic security partnership:

- Risk should involve the CISO team (and where appropriate the CIO team) in setting policy, to give them insight into enterprise risks and gain their buy-in to cyberrisk policies.

- The risk team should collaborate with the teams of the CISO and CIO to create targets for key risk indicators that are well within the enterprise risk appetite. With input from the CISO and the CIO, risk decides what should be measured and reports to executive leaders and the board on the status of the targets.

- Risk becomes an active partner in helping the CISO identify and clear barriers to implementation across the organization, especially within the business.

- Risk promotes the program to reduce cyberrisk that has been created jointly by the teams of the CISO, CIO, and CRO. The sense of shared objectives will increase the program's momentum and help measure and report on risk-appetite boundaries more effectively.

be given the authority to push respective teams for data and information needed to complete tasks on time. It is helpful if these decision makers from each organization meet regularly throughout the year as a working group. This will help build working camaraderie, keep the group abreast of changes, and magnify the focus on the common goal of reducing the institution's top cyberrisks.

With cyberthreats mounting in number and sophistication, large institutions can no longer protect against all risks equally. The threats posing the most danger to the business must be identified and neutralized first. For this to happen, the risk function must be deeply embedded in cybersecurity planning and operations. That is what the strategic-security-partnership model is all about. ■

Oliver Bevan is an associate partner in McKinsey's Chicago office; **Jim Boehm** is an expert associate partner in the Washington, DC, office; **Merlina Manocaran** is a partner in the New York office; and **Rolf Riemenschnitter** is a partner in the Frankfurt office.