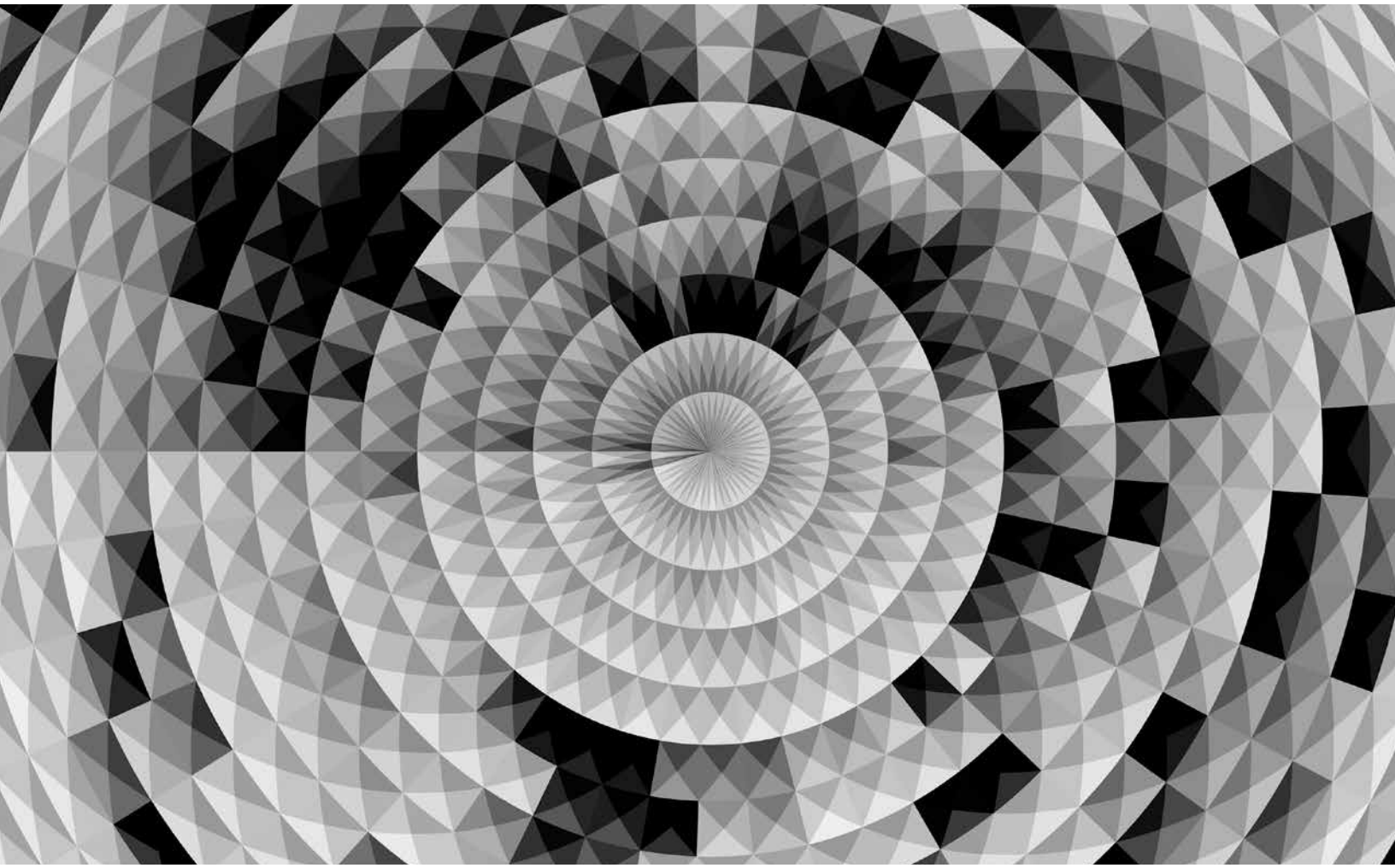
Cyber risk measurement and the holistic cybersecurity approach

Comprehensive dashboards can accurately identify, size, and prioritize cyberthreats. Here is how to build them.

Jim Boehm, Peter Merrath, Thomas Poppensieker, Rolf Riemenschnitter, and Tobias Stähle



NOVEMBER 2018 • RISK PRACTICE

Damaging cyberattacks and streams of suspicious digital communications have made cybersecurity a top concern of the world's business leaders. So say the overwhelming majority of responding board members in a recent McKinsey survey. Their answers are further evidence that cyber risk is now as important a priority for the leaders of public and private institutions as financial and legal risks.[1] Facing a rising threat level and the magnitude of the potential impact, executives are insisting on full transparency around cyber risk and ways to manage it actively to protect their organizations.

This evolved attitude was also expressed in the responses to our recent article, "A new posture for cybersecurity in a networked world."[2] Most readers who commented agreed on the urgency of the issue, and many volunteered stories of rising cyberthreats, new types of attacks, and the increasing complexity of managing digital risk in large corporations. A board member for a multinational company in advanced industries admitted, "So far, we have not taken a big hit, but I can't help feeling that we have been lucky. We really need to ramp up our defenses." Another executive said: "Digital resilience is one of our top priorities. But we haven't agreed on what to do to achieve it." These concerns are widely held, as executives in all sectors and regions seek guidance on the path to a new cybersecure posture.

Board members and their discontents

Survey responses revealed that companies are rolling out a wide range of activities to counter cyber risk. They are investing in capability building, new roles, external advisers, and control systems. What they lack, however, is an effective, integrated approach to cyber risk management and reporting. As top executives attest, these tools are urgently needed to support fast, fact-based cyber risk management. There are three specific gaps:

- *Lack of structure.* Boards and committees are swamped with reports, including dozens of key performance indicators and key risk indicators (KRIs). The reports are often poorly structured, however, with inconsistent and usually too-high levels of detail. Research indicates that most IT and security executives use manually compiled spreadsheets to report cyber risk data to their boards; unsurprisingly, many board members are dissatisfied with the reports they receive.[3]

- *Lack of clarity.* Most reporting fails to convey the implications of risk levels for business processes. Board members find these reports off-putting—poorly written and overloaded with acronyms and technical shorthand. They consequently struggle to get a sense of the overall risk status of the organization. At a recent cybersecurity event, a top executive said: "I wish I had a handheld translator, the kind they use in *Star Trek*, to translate what CIOs [chief information officers] and CISOs [chief information security officers] tell me into understandable English." In a recent survey, 54 percent of executives said that risk reports are too technical.

- *Lack of consistent real-time data.* Different groups in the same organization often use different, potentially conflicting information to describe or evaluate the same aspects of cyber risk. An executive remarked that one day he received a report listing an asset as sufficiently protected, but the next day a different department reported the same asset as under threat. "Which should I believe?" he asked, "and what should I do?" To compound the problem of conflicting reporting, underlying data are often too dated to be of use in managing quickly evolving cyberthreats.

A holistic strategy

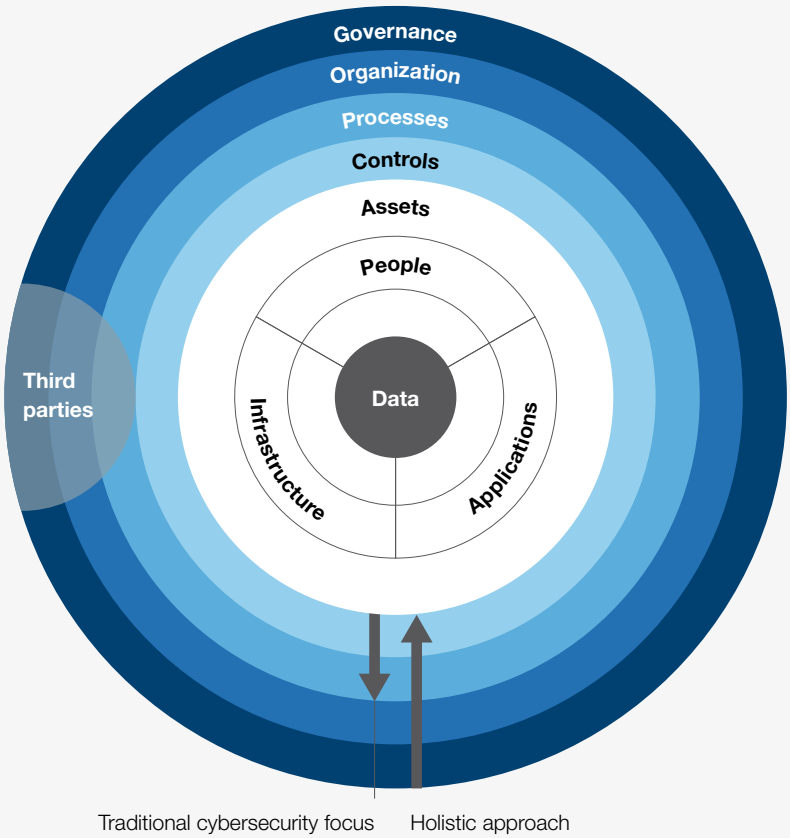
A holistic approach to cybersecurity can address these failings and their implications for governance, organizational structures, and processes (Exhibit 1).

A holistic approach proceeds from an accurate overview of the risk landscape—a governing principle that first of all requires accurate risk reporting. The goal is to empower organizations to focus their defenses on the most likely and most threatening cyber risk scenarios, achieving a balance between effective resilience and efficient operations. Tight controls are applied only to the most crucial assets. The holistic approach lays out a path to root-cause mitigation in four phases (Exhibit 2).

1. Identify risks and risk appetite. Working with top management and drawing on internal and external resources, the chief risk and information security officers create a list of critical assets, known risks, and potential new risks. In conjunction with this

Exhibit 1 **The holistic approach to managing cyber risk proceeds from a top-management overview of the enterprise and its multilayered risk landscape.**

Holistic cyber risk–management approach



Assets. Clearly defined critical assets

Controls. Differentiated controls to balance security with agility

Processes. State-of-the-art cybersecurity processes focused on effective responses

Organization. Right skills, efficient decision making, and effective enterprise-wide cooperation

Governance. Investments in operational resilience prioritized based on deep transparency into cyber risks

Third parties. Coverage of the whole value chain, including third-party services

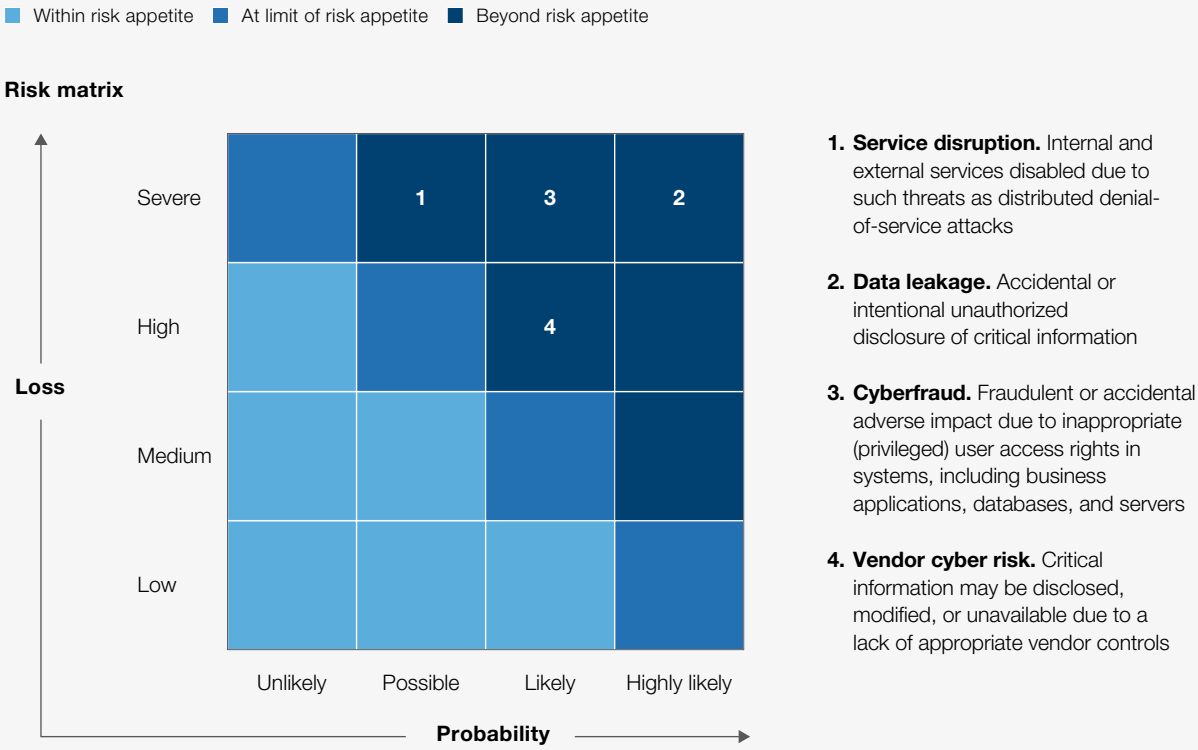
Exhibit 2 **The holistic approach lays out a path to root-cause mitigation of top risks in four phases.**

effort, top management and the board establish the organization's appetite for the risks that have been identified. An assessment is also made in this phase of existing controls and vulnerabilities. The risk appetite will vary according to the value to the organization of the threatened asset. A leaked internal newsletter, for example, is less likely to pose a serious threat than the exposure of customer credit-card data. The chief measure of cyber-resilience is the security of the organization's most valuable assets. The prioritization of identified risks is therefore a task of utmost importance, which is why top management must be involved.

2. Analysis and evaluation. Once the risks and threats have been identified, internal and external experts need to evaluate each risk with regard to likelihood of occurrence and potential impact, including, as applicable, regulatory, reputational, operational, and financial impact (Exhibit 3).

Exhibit 3

Each identified risk is evaluated with regard to potential loss and likelihood of occurrence; a matrix displays resulting prioritized threats.



Based on this assessment, the risk function or risk owners can prioritize areas for mitigation, starting with the most likely scenarios that will have the biggest negative impact (top right-hand area of the map, marked in dark blue in the exhibit).

3. Treatment. Once risks have been identified and prioritized according to likelihood and impact, the risk owners and the risk function should work together to create an overview of all initiatives undertaken to mitigate the top cyber risks. The initiatives should be evaluated on their effectiveness in reducing the probability of a risk event occurring and the impact of an event that does occur. Taking into account the effects of the mitigating initiatives, risk experts determine whether the residual risk for each top risk now falls within the parameters of the organization's risk appetite. Should the residual risk level exceed these considered limits, additional mitigation initiatives can then be developed and deployed.

4. Monitoring. Among the most important instruments for fostering discipline throughout the organization are scheduled status updates to senior management on top cyber risks, treatment strategy, and remediation. Over time, the indicators and criteria used in such updates will become the basic language in the organization's conversations about risk. The updates should be well written, concise,

and free of mysterious acronyms and specialized jargon. For the board, a single well-composed page of text should suffice.

Focused risk mitigation

Cyber risk managers in large organizations are often swamped with information on threats that exceeds their capacity to respond appropriately. Fortunately, not all the alerts are warranted. For example, most organizations are little threatened by a so-called advanced persistent attack. The low probability should become visible in risk analysis, freeing organizations from devoting resources to the highly sophisticated defenses needed to protect against such attacks. Instead, they will be able to focus on creating countermeasures for common kinds of attacks—such as, for example, a distributed denial of service induced by malware or malicious overload. The optimal strategy will include controls to prevent collateral damage and investment in state-of-the-art safeguards to ensure business continuity in case of an attack. The goal for cyber risk managers is an efficient, adaptive, and sustainable regime. To attain it, fact-based prioritization is of great importance. Accurate risk sizing is dependent on a few basic inputs:

- a business perspective of the institution's key assets and the top risks that could affect them
- realistic updated assessments of relevant threats and threat actors, formulated in detail as appropriate
- a consistent and accurate definition of risk appetite for the organization as a whole, prioritized and revised as appropriate

With an approach based on these factors, executives can give clear guidance on cyber risk to all levels of the organization. The overall strategy includes a well-prioritized risk profile, efficiently focused on reducing disruption or slowdowns. For example, employee-related controls would be tailored by role—controls to avoid data leakage would apply only to those with access to key assets, rather than to all.

Resolving the data dilemma

Most companies are wary of their operational data sources and often assign risk, compliance, or control teams to build additional data sources or clean existing operational data. This response to one problem often creates a number of others. It expends substantial resources and leads to different, inconsistent reports as well as a growing reservoir of "stale" data from past risk-assessment efforts. Yet when specific questions arise, needed data cannot be located and appropriate action cannot be taken. Risk teams must scramble to dig up the data manually, double-check facts, and conduct interviews to discover what is really going on. As the head of cyber risk for an insurance company remarked, "We spend half our time looking for data and aggregating information from different sources."

Integrated data architecture and a consolidated data lake

Consistent cyber risk reporting is an essential part of the response to the everyday demands of cybersecurity. To achieve a state of readiness against cyberattacks, companies need to build an integrated data architecture, including a consolidated data lake. To avoid conflicting, inconsistent information, the data lake should be filled directly from an organization's "golden sources" of data on vendors, people, applications, infrastructure, and databases. All data corrections need to be made to these original sources in a consistent manner, covering all relevant assets.

By enforcing data consistency, companies will help foster cyber risk consciousness. Those charged with gathering, cleaning, and processing data are actually contributing to a cybersecurity transformation. One financial-services executive explained:

> *Initially, we created a data lake with an off-the-shelf interface, assuming the organization would figure out what to use it for. We failed miserably. Very few people used it at all, and everybody else tried to prove the output wrong. Now we work with our most experienced people to outline the benefits and build our data regime one use case at a time. To want to work with data, people need to see how data can make their life easier and their business more resilient.*

To ensure continuous, consistent, accurate, and timely cyber risk reporting, the level of automation in data gathering and processing should be increased gradually, step by step. Areas such as asset identification and compliance monitoring can be tackled in sequence. Automation can help improve data quality; advanced analytics and machine learning can find empty cells, missing pieces, and suspicious patterns in the underlying data. Automated pattern hunting is especially effective in verifying the quality of external data sources, from partners along the value chain, for example, or from specialized providers of risk-related data.

Holistic cyber risk reporting

When risk managers set out to implement holistic cyber risk reporting, they are often surprised by how little they know about their organization. Many organizations have no reliable inventory of databases, applications, devices, people, buildings, third parties, and access rights. At many companies, vulnerable critical assets are managed locally, invisible to cyber risk managers at company headquarters. At one financial-services firm, as many as 50 copies of the same data were being held, including for highly sensitive customer information. While some of the copies were well protected with state-of-the-art controls, others floated around and were frequently transferred using unencrypted email and even employees' personal thumb drives. Although strict controls had been defined, business units granted exceptions from the rules in a parallel process that was not aligned with the overall digital risk-management regime. This double standard was a major source of uncontrolled risk for the whole organization.

At a large manufacturer, critical industrial-production environments were connected to the internet through unregistered interfaces. These had been installed by third-party providers for remote maintenance. In effect, they exposed the entire production environment to cyberattacks. The scope of such attacks has lately extended beyond IT systems to operational technology (OT). OT systems include industrial control systems and Internet of Things devices, from refrigeration units to pacemakers. Such equipment is often more vulnerable than IT systems because OT security standards are less developed. The lesson from the experience of OT vulnerability is that all critical assets must be part of the cybersecurity strategy. The strategy must cover the entire value chain, minimizing the blind spots of an organization's risk assessment.

Visualizing threat control: The cyber risk dashboard

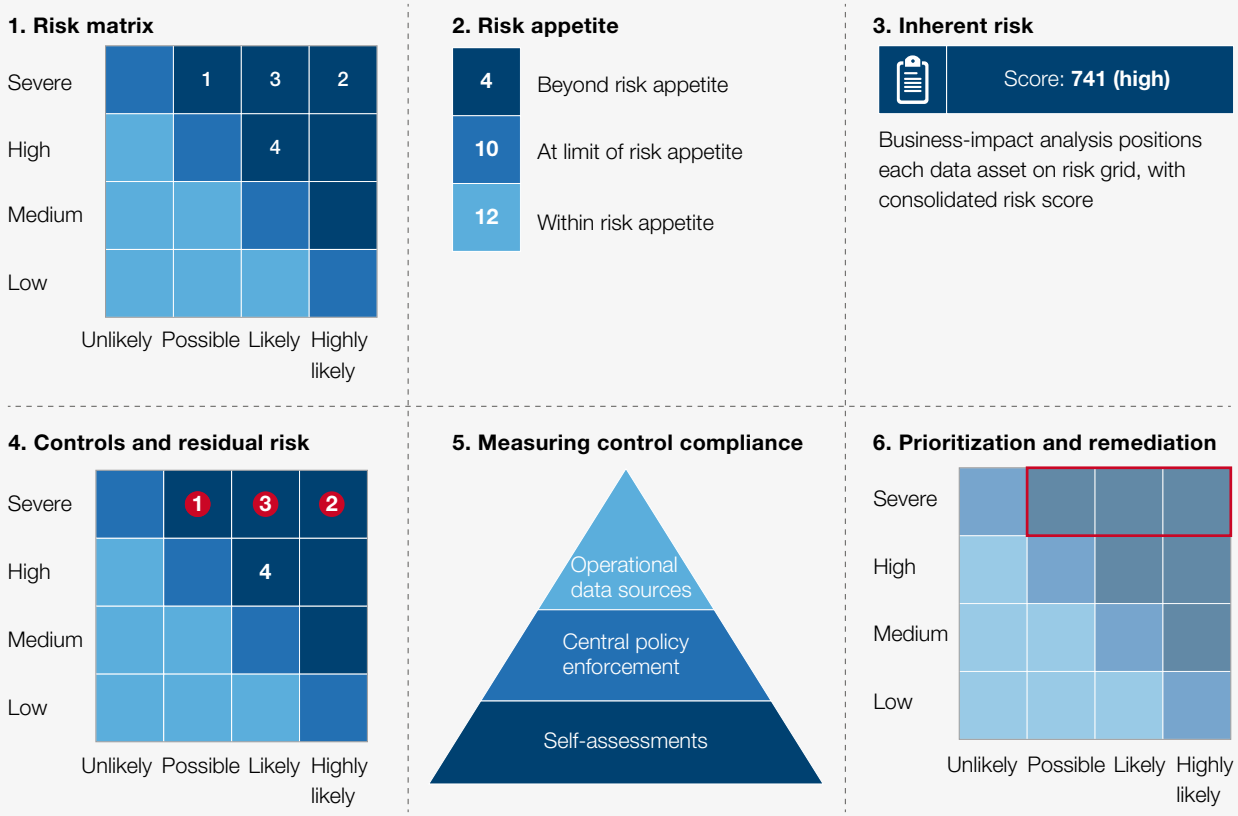
Leading companies include progress updates in their cyber risk reporting. The updates provide information on the status of counter-risk initiatives and

the changing threat landscape. To make information most accessible to decision makers, dashboards for cyber risk are needed. These instrument panels allow nonspecialists to readily scan the crucial data (Exhibit 4). A good dashboard can summarize the entire risk-management terrain in a series of dynamic panels, presenting the following analyses:

- the evolution of the relevant threat landscape and its implications for the organization
- an overview of recent cyber risk events, incident development, and key countermeasures taken
- the top cyber risks as defined in cooperation with the business units and measured through clearly defined key risk indicators
- risk assessments in light of clearly defined risk appetites, with recommendations on the assets in need of prioritized attention (see sidebar "Prioritizing counter-risk initiatives according to the value at risk")
- a detailed plan of the counter-risk initiatives in place, with relevant accountabilities, implementation status, and actual impact on risk reduction

Exhibit 4 **The cyber risk dashboard displays end-to-end risk monitoring and management in real time, enhancing executive control.**

Cyber risk dashboard, illustrative



To support effective decision making, optimally designed dashboards allow users to drill down from group-level risk status to individual businesses and legal entities—and finally to the vulnerable assets underlying particular threats. Experience with risk dashboards demonstrates that decision makers need to view all pertinent KRIs, for individual assets as well as the business unit as a whole. KRI views should be adapted to individual roles: business-unit managers should be able to view only KRIs related to their own business unit, while the chief information officer (CIO) or chief risk officer (CRO) should be able to aggregate the dashboard output across business units, functions, and entities.

The cyber risk dashboard metrics must accurately measure actual risk levels. Their purpose is to enable better, faster decisions to avert threats and increase an organization's overall resilience. The dashboard must be built upon data that are relevant, up to date, vetted for quality, and aggregated in meaningful ways. Integrated data from trusted sources, frequent updates, and analytical capabilities allow decision makers to derive meaningful insights directly from a dashboard. They are provided with the facts they need to fight against digital attacks, fraud, and blackmail. It is best understood as the most visible part of an integrated data and analytics platform for holistic digital risk management (Exhibit 5).

How dashboards enable better decision making

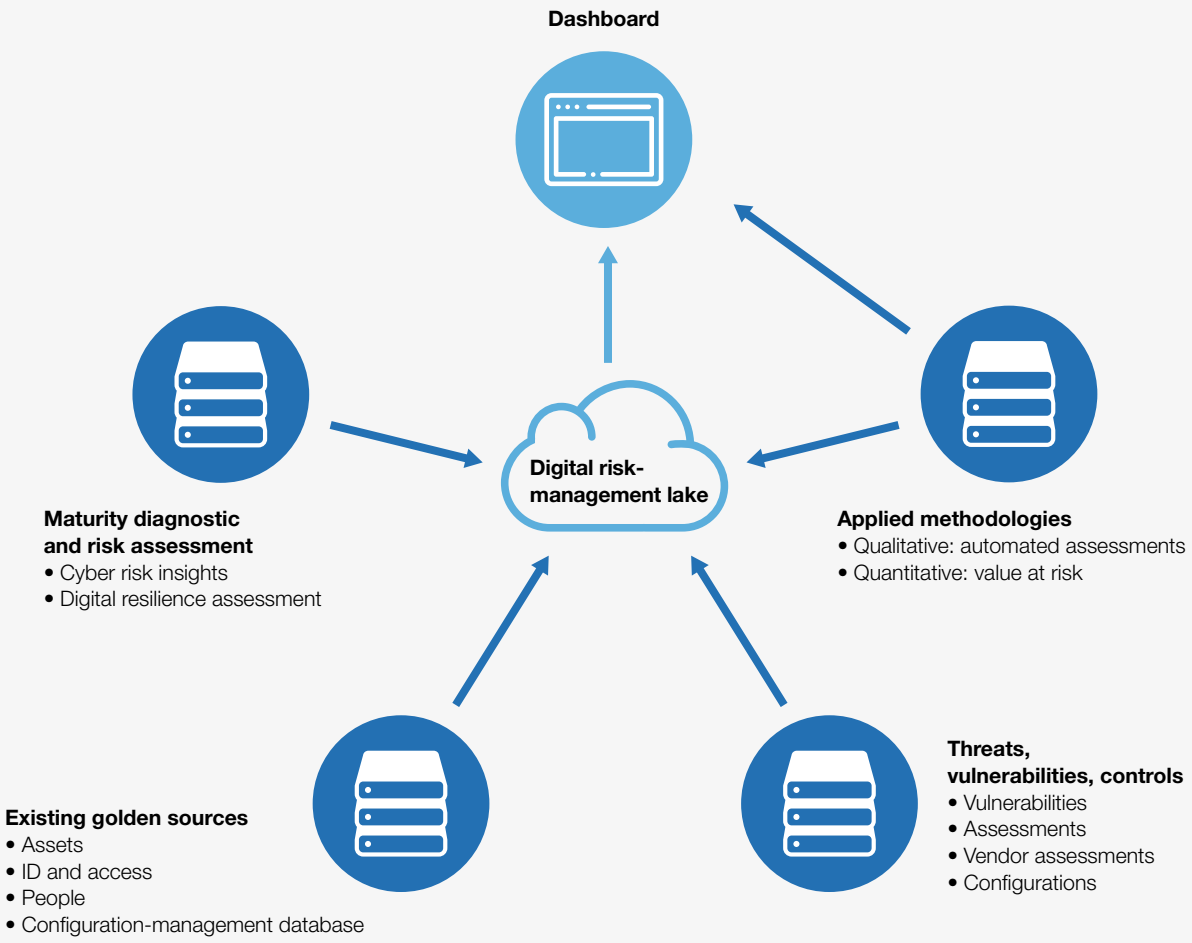
A good cyber risk dashboard is one designed to promote good decision making. One way it does this is by simplifying details, intricate KRIs, and complicated visuals to communicate the most essential information—an essentially complete risk profile. An executive in the financial-services industry explained the advantages of a relatively simple dashboard:

> *Before we had a cyber risk dashboard, we implemented cyber risk controls more or less at random. Everything was important. We tried to protect all assets with middle-of-the-road controls. As a result, we were spread too thinly in some critical areas, such as private-banking applications. At the same time, we were going overboard with cumbersome controls in other, less critical areas. What the dashboard helped us do was focus our efforts and our investments. We were able to limit the scope of the [heavy controls], such as advanced encryption and two-factor authentication, to crucial, high-risk assets. As a result, we are now better protected than before, while our operations run much more smoothly.*

Over the course of dozens of cybersecurity transformations, we have found that almost all companies systematically overinvest in the protection of virtually risk-free assets, while the protection of high-risk assets is often underfunded

To support effective decision making, optimally designed dashboards allow users to drill down from group-level risk status to individual businesses and legal entities.

Exhibit 5 **A digital risk dashboard is the most visible part of an integrated data and analytics platform for holistic digital risk management.**



or undermanaged. A good cyber risk dashboard provides the kind of information that will help risk managers rebalance the scales and focus their resources on averting the biggest threats to the organization's most critical assets. As another executive remarked:

> *Implementing controls for everything is the easy way, but it's ultimately too expensive, and it slows us down too much. You have to pick your battles, in line with your company's risk appetite. But you need a reliable fact base. Only then can you decide not only for but also against the implementation of controls and still sleep soundly.*

While the benefits of a cyber risk dashboard may be obvious, the challenges only become apparent when companies begin to put holistic cyber risk management into practice.

Overcoming blind activism

A good dashboard promotes resilience and efficiency; an unsuitable dashboard does the opposite. At worst, it might deceive decision

Prioritizing counter-risk initiatives according to the value at risk

Consolidated information about threats, vulnerabilities, and an organization's cyber resilience is a powerful lever in its own right. Consolidation creates transparency, awareness, and discipline around the ways an organization understands and manages risk. But this information becomes even more powerful when it is combined with information about critical business processes and the losses incurred under adverse scenarios—such as a temporary suspension in service. The combination of risk and business data allows risk managers to calculate the value at risk in a given area and accordingly prioritize counter-risk initiatives. This means that the organization is directing available resources toward its most pressing material risks. Prioritization is especially important as the scope of risk-management increases. In the financial-services industry, most risk managers we surveyed said that they expect to take on more comprehensive responsibilities in the future. Given the coming risk burdens, companies will need to invest in an integrated data and analytics platform that drives fast, fact-based decision making. For more details, see our recent report *The future of risk management in the digital era*, created in collaboration with the Institute of International Finance, on Mckinsey.com.

makers about threats and controls, leaving the organization more vulnerable than it appears. Poorly performing dashboards can trigger blind activism, with red flags going up all the time. Misleading alarms can be set off by an inarticulate risk appetite, excessively cautious managerial self-assessments, poor data quality, undifferentiated controls across all assets, and inadequate alert thresholds.

When alarms are near constant, response teams are always in firefighting mode and risk managers and IT and OT security experts are always overloaded with work. Blind activism increases stress on entire organizations but rarely increases resilience. For that, the organization needs effective cyber risk governance structures. These are best supported by a well-constructed dashboard reflecting the risk appetite and fed with consistent data from golden sources. These tools will bring transparency and resilience and also do wonders for efficiency and employee motivation. Fact-based prioritization will help focus an organization's efforts on fighting cyber risks in the top right-hand quadrant of the risk heat map: those that are most serious and likely to occur.

Conversely, controls for risks nearer the bottom left-hand quadrant (less threatening, less likely) can be loosened or discontinued to free up resources. Before long, the organization will have moved from a blind, undifferentiated compliance focus to one in which controls and business-continuity-management processes are based on robust facts about actual risks.

Building a good dashboard is not, or at least not primarily, about coding. It is more the result of

engaged conversations across roles in which acceptable risks are identified, the data needed to understand the organization's true resilience are marshalled, and the focal points for risk-reducing investment are established, along with the most effective ways to monitor progress.

Breaking down silos

In our experience, silos—isolated functional units and the disconnected thinking they foster—are one of the biggest obstacles to cyber risk transformations. At many institutions, data owners and line managers confine themselves to only

Application examples and voices from the C-suite

ROI-based cyber risk management and advanced control implementation in healthcare

Healthcare is among the most risk-sensitive industries because of the trove of patient data and financial information it generates, stores, and processes on a daily basis. The chief information officer (CIO) of a health-insurance provider sought to put the company's cybersecurity funds to optimal use. The governing objective was to reduce overall risk and implement advanced capabilities to counter evolving threats. Historically, the company had been focused on compliance with high-level regulatory requirements. Existing controls were undifferentiated, and the CIO was concerned that her investments were not effectively prioritized from a return-on-investment (ROI) perspective. In response, the board members, relying upon a customized probability–loss matrix, determined the most critical assets as well as the acceptable risk levels for each (risk appetite). In a second step, the company was able to reallocate 20 percent of its total investment in a multiyear cybersecurity program (exceeding $100 million) from routine activities, such as penetration testing, to advanced controls for highly critical assets.

We now have the financial leeway to build out our next-generation security-operations center and an insider-threat program. Thanks to the new approach, we are definitely getting more value for our money than before.
—Healthcare CIO

Reducing the value at risk with improved business-continuity management in consumer goods

Alerted by the proliferation of computer viruses, untargeted malware, and attacks on production systems, a consumer-goods manufacturer decided to ramp up its cyber risk reporting and management regime. The company took a holistic risk-monitoring and management approach. Specifically, the CIO enhanced the company's business-continuity management. The primary objectives were to reduce the value at risk in core processes and to assign the company's cybersecurity resources according to a risk-based approach, leveraging operational data. In effect, the company put its limited resources and maintenance windows to much better use than under the previous regime. Investments in controls and responses are now focused on the most critical,

that part of the data pool, organization, or value chain for which they are responsible. They are not required to look left or right and by design cannot see the big picture. They are therefore unable to make the choices needed to balance resilience with smooth operations. Data owners often hesitate to share what they own, and line managers often feel burdened by the need to comply with risk-management guidelines. As one data owner put it, "If I give up my data, what do I have left? The data is what makes me relevant to the company." A line manager said, "All these controls slow me down.

most vulnerable applications, such as the system that steers the supply chain and the browser-based interface to distribution partners. To increase resilience even further, the company's IT and HR departments set up an online training program that helps employees handling critical systems spot signs of cyberattacks at an early stage. The company's key informational and operational assets are now much better protected than before.

The new reporting has significantly reduced our risk of becoming the victim of an untargeted attack.
—Consumer-goods CIO

Enhanced risk-appetite setting and streamlined cyber risk reporting in financial services

The chief risk officer (CRO) of a global bank complained that the company's cyber risk reporting was outdated and inconsistent across the different lines of defense. Frequently, the board and regulators were presented with conflicting messages about threats and increasingly impatient requests for responses from multiple stakeholders. "We have had complaints from regulators in three different countries. The supervisory board is breathing down my neck," the CRO remarked. The bank in fact held no common understanding of cyber risk nor consensus about acceptable risk levels. The CRO, the chief operating officer, and business-unit leaders decided to develop a consistent cyber risk scorecard focused on the top 15 cyber risks, a consolidated set of key risk indicators, an enterprise-wide definition of risk appetite, and selected key performance indicators to measure the success of the bank's investments in cybersecurity. An additional benefit of these enhancements was that the digitization they required also freed up significant team resources that had been assigned to generating reports.

For the first time, we have real transparency and consistency in how we manage cyber risk. The scorecard is fully digitized. I can bring it up on my tablet any time. When nervous members of the supervisory board or regulators call me, I have all the information I need to answer their questions. In most cases, I can tell them right away what we are doing to fight the threat they have read about in the paper. And instead of wasting time debating inconsistencies, my direct reports now have the time to develop recommendations for better controls.
—Financial-services CRO

Why should I cooperate with the cyber risk team if all they do is make my life more difficult?" The reports emanating from an organization of siloed thinkers will frustrate decision makers, one of whom complained, "Why do I need to look at all these moon phases and traffic lights? How do all these indicators relate to our business? What I need to know is whether our top assets are protected, and what I should do if they are not."

A good dashboard can help break down the silos, by bringing together different kinds of people—from detail-oriented database managers to top executives with short attention spans. To create a good dashboard the group needs to collaborate, as all will eventually benefit from its output. The dashboard forces all to adopt a common language, one that harmonizes definitions of KRIs, criticality, threat levels, and compliance (for further insight, see sidebar "Application examples and voices from the C-suite").

Neither groups of technical wizards nor teams of business specialists could accomplish the needed transformation on their own. For that, the diverse group of interested parties—business owners, programmers, data scientists, designers, change managers, and privacy lawyers—must be made to relate to one another regularly. Only then will the business implications of the technology, as well as the technological requirements of the business goals, be reciprocally understood. The culture will transform itself once these many roles, with their rich collective expertise, rediscover their common purpose.

Establishing holistic cyber risk reporting and governance is as much about people as it is about processes and dashboards. In the most successful transformations, consistent reporting acted as a catalyst of cultural change. At first sight, a dashboard may appear to be a piece of software with a fancy front end. In truth, it is the material expression of the agreed-upon KRIs, aggregation levels, and reporting cycles. The discussions that lead to these agreements are change agents in their own right. Two further lessons of successful transformations are worth underlining: involve business owners from day one and be willing to make trade-offs to find the right balance between protection and productivity. To help them with these decisions, executives will find experienced managers, who will then become the abiding advocates of the new holistic approach.

[1] McKinsey global survey of 1,125 board members of leading companies in all industries, April 2017. Seventy-five percent of respondents included cybersecurity among the top five board concerns.

[2] *McKinsey on Risk* Number 5, June 2018, McKinsey.com.

[3] Osterman Research, ostermanresearch.com.

Jim Boehm is an associate partner in McKinsey's Washington, DC, office; **Peter Merrath** is an associate partner in the Frankfurt office, where **Rolf Riemenschnitter** is a partner and **Tobias Stähle** is a senior expert; **Thomas Poppensieker** is a senior partner in the Munich office.