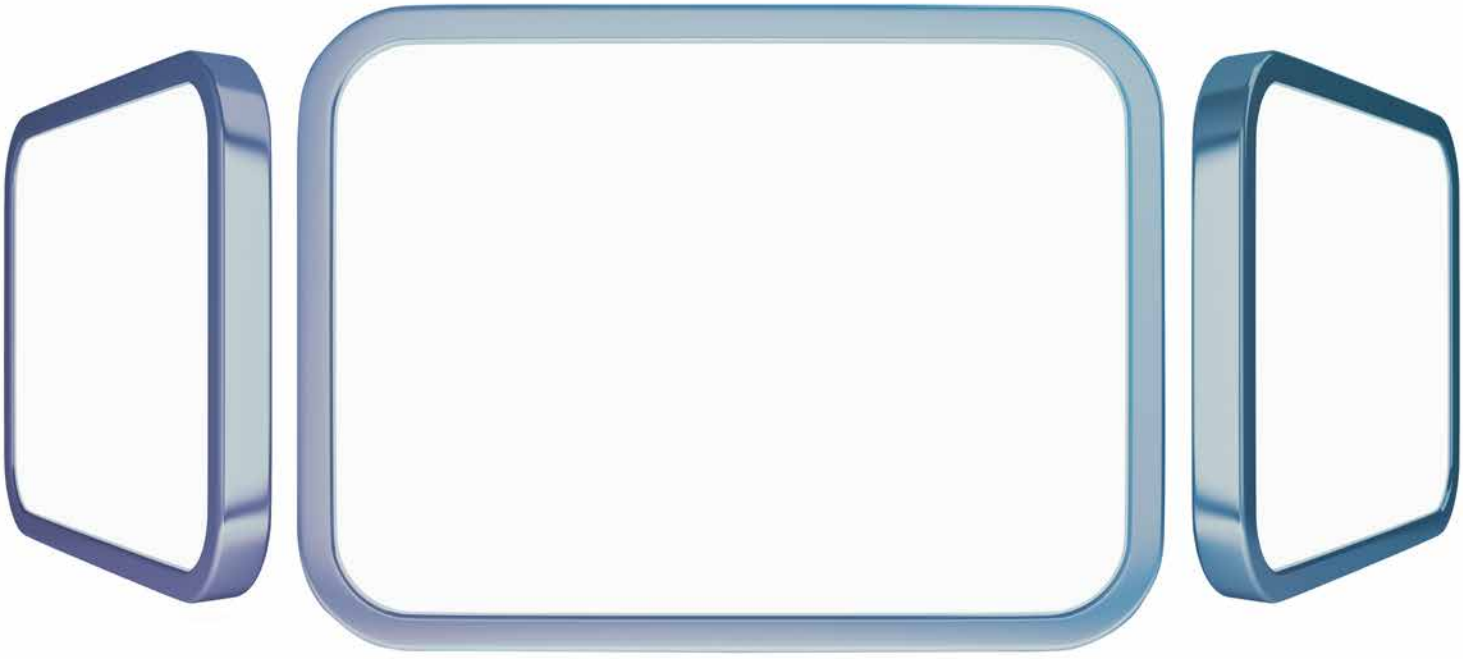
McKinsey & Company

Risk Practice

Enhanced cyberrisk reporting: Opening doors to risk-based cybersecurity

New cyberrisk management information systems provide executives with the risk transparency they need to transform organizational cyberresilience.

by Jim Boehm, James M. Kaplan, Peter Merrath, Thomas Poppensieker, and Tobias Stähle



January 2020

Executives in all sectors have deepened their understanding of the dangers cyberrisk poses to their business. As hacks, cyberattacks, and data leaks proliferate in industry after industry, a holistic, enterprise-wide approach to cybersecurity has become a priority on board agendas. Companies are strengthening protections around their business models, core processes, and sensitive data. Regulators are applying their own pressures, and privacy demands are sharpening.

We asked executives at financial institutions in Europe and North America about their actual experiences with cyberrisk management and reporting. What they told us was instructive. They said cyberrisk management can be effective only when the information it is based on is accurate. Yet cyberrisk reporting at many companies is inadequate, failing to provide executives with the facts they need to make informed decisions about countermeasures. Because of the information gaps, managers often apply a standard set of controls to all company assets. As a result, low-priority assets can be overprotected, while critical assets remain dangerously exposed.

Fortunately, some leading organizations are pioneering an effective, efficient approach to cyberrisk reporting that helps executives increase corporate resilience—one that also provides transparency on cyberrisk and allows companies to integrate cyberrisk reporting with legacy systems.

Risk managers are flying blind

Many companies rely on a patchwork of reports from different sources to manage cyberrisk. Executives at these companies are unable to assess the return from their cybersecurity investments. They lack needed information about cyberrisk levels, the effectiveness of countermeasures, and the status of protection for key assets. Available data are incomplete, inconsistent, and not reliable as a basis for decision making. Executives also question the complexity of their cyberrisk-management tools, finding them overly complicated and their results incomprehensible.

Risk decision makers reserve particular criticism for governance-risk-compliance (GRC) systems. These complex software solutions can take years to implement and rarely produce a satisfying result. Like many risk-management systems, GRC software was created by technicians, and specialized expertise is required to make sense of the output. In one survey, more than half of executive respondents said cybersecurity reporting was too technical for their purposes.[1] In fact, GRC does not even focus on cyberrisk but rather covers a wide range of risk types,

[1] *How boards of directors really feel about cyber security reports*, Bay Dynamics, June 2016, baydynamics.com.

> "We need to bring rigor to the risks related to data and protect our top assets effectively."
>
> —Advanced industries CIO

> **"The current situation is a mess. We do not have the facts to decide on actions. This paralysis puts our business at risk."**
>
> **—Financial-services chief information-security officer**

including financial, legal, natural, and regulatory risks. It therefore cannot create the overview of cybersecurity that board members and regulators need. In effect, many cyberrisk managers are flying blind.

At a leading European financial institution, executives were dissatisfied with the existing cyberrisk-reporting regime. In attempting to improve it, they first assessed their experience:

— Cyberrisk reports were compiled by IT specialists for other IT specialists. As a result, the reports were very technical in nature and provided little to no guidance for executive decision making. Executives found that the reports did not help them interpret how cyberrisk is related to other risks the institution faces, such as legal or financial risks.

— At the same time, the reporting had many gaps: almost no information was provided on top risks, key assets, recent incidents, counter-risk measures, implementation accountability, the institution's resilience in the face of cyberthreats, or the return on investments in cybersecurity.

— The reporting was structured by systems, servers, and applications rather than by business units, business processes, functions, countries, or legal entities. Most reports were compiled as stand-alone documents, with no integrated view of cyberrisk across the group .

The executives had no clear sense of the overall magnitude of the risk from cyberattacks, malware, and data leaks. Neither did they know what was needed to improve protection of their key assets against the biggest threats. Several mitigating initiatives were in progress, but the reporting did not make clear what contributions if any these actions made to reducing risk. Cyberrisk managers found it difficult to decide on the areas of focus for cybersecurity investments or to justify their ultimate decisions to the board. For want of reliable reporting, the entire cybersecurity strategy was undifferentiated: all controls were being applied to all assets.

The chief information-security officer (CISO) did not know whom to contact about a given issue. Regulators reproached the institution for incomplete information. For example, the institution did not compile data on the share of employees that had completed mandatory cybersecurity training in any one location. Within the undifferentiated group-level data, high attendance in one country could easily mask low attendance in another. The training gap could be contributing to unacceptable levels of cyberrisk exposure in that country, which, however, would be invisible.

The objectives of effective cyberrisk reporting

State-of-the-art cyberrisk management requires an information system that consolidates all relevant information in one place. The most important risk metrics—key risk indicators (KRIs)—present a consistent evaluation across assets to enable the tailored application of cyberrisk controls. A given asset can be protected with the controls appropriate to its importance and the threat levels to which it is exposed.

To ready their companies for the challenges of the evolving cyberrisk-threat landscape, executives need to upgrade their approach to cyberrisk reporting and management. To address the magnitude and the complexity of the threat, companies should build a high-performing cyberrisk management information system (MIS) with three fundamental objectives.[2]

— Transparency on cyberrisk. Make the cyberrisk status of the institution's most valuable assets fully transparent, with data on the most dangerous threats and most important defenses assembled in a way that's accessible and comprehensible for nonspecialists.

— Risk-based enterprise overview. Provide decision makers with a risk-based overview of the institution so they can focus their cybersecurity investments on protecting the most valuable assets from the most dangerous threats.

— Return on cyber investments. Ensure the efficiency of counterrisk measures by requiring a high return on investment.

A dedicated cyberrisk MIS is not a substitute for GRC systems but rather a reporting solution addressing cyberrisk. It must be compatible with legacy systems and serve decision makers rather than specialists. It is designed to provide the information that executives need to prioritize threats and devise effective controls; it enables informed board discussions on cyberrisk strategy and helps optimize the allocation of funds.

The cyberrisk MIS should not become a burden on executives, reduced to yet another software system they must learn. Rather, it should be integrated into the existing business-intelligence system, drawing initially on existing data sources. A good cyberrisk MIS should also aspire to be future-proof, adaptable to new technologies, and able to integrate more granular data sources and more sophisticated algorithms for risk assessment as they become available.

For optimal performance, the cyberrisk MIS should be tailored to the needs of a given company. However, even a basic setup can create substantial impact. This is because a cyberrisk MIS acts as a catalyst for better, more informed decision making. Even the process of setting it up forces executives to come to a common understanding of the level of cyberrisk the company is willing to tolerate.

A strong analytical backbone

Analytics is the backbone of the cyberrisk MIS; having a strong, smart analytical system in place enables users to integrate data from different sources across a network and aggregate risks as needed. Ideally, the cyberrisk MIS should have a pyramid structure, with risk data organized hierarchically. The starting point is a simple overview, with the most important data at the highest level of aggregation. These data would describe, for example, the top global risks, differentiated by potential loss and probability. More detailed information can be added as needed, including KRIs and countermeasures for individual divisions, countries, assets, processes, and even buildings. The contact details of the people responsible for implementing the specific countermeasures can also be included.

[2] See also Thomas Poppensieker and Rolf Riemenschnitter, "A new posture for cybersecurity in a networked world," *McKinsey on Risk*, March 2018, McKinsey.com.

As shown in Exhibit 1, a top-down approach for risk-data aggregation typically involves the use of qualitative risk assessments based on scenarios. Top down is a good way to begin: it requires the least amount of data and provides significant insight in a short time. Eventually, enough risk data will become available to introduce a bottom-up approach.

The movement from top down to bottom up helps achieve cyberrisk MIS objectives quicker—by clarifying definitions of the elements of cyberrisk, providing executives with the information they need to make strategic decisions, and enhancing transparency on risk exposure and the efficacy of risk-mitigation initiatives.

Exhibit 1

The cyberrisk management information system begins with top-down risk aggregation and proceeds to a bottom-up approach.

Risk management and reporting

Low in risk appetite | In risk appetite | At risk appetite | Out of risk appetite

Top-down risk aggregation is a good way to begin, as it requires the least amount of data and provides the most insight in the shortest time

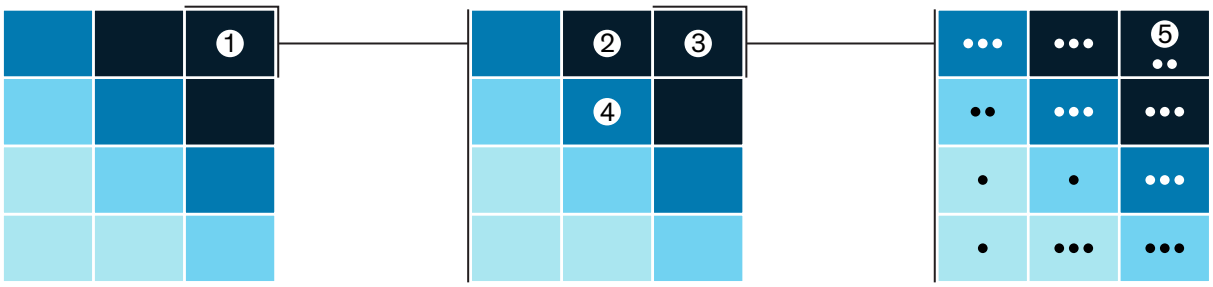
Methodologies
- Scenario-based, qualitive and quantitative assessments

The top-down risk approach is phased into a bottom-up approach as the organization matures and the required data become available

Methodologies
- Scenario-based, qualitive, and quantitative assessments
- Operational-risk-management (ORM) methodologies and portfolio-theory aggregation

The bottom-up approach allows for more effective risk mitigation: it provides transparency sufficient to achieve optimal risk-treatment decisions for a given budget in line with enterprise capabilities

Methodologies
- Business-impact analysis
- Inherent and residual risk exposure
- Risk-inheritance modeling
- ORM methodologies and portfolio-theory aggregation
- Low-level data processing



1 Group enterprise-information risk exposure

2 Data-confidentiality breach
3 Data-integrity loss
4 Insufficient technical-disaster recovery

5 Risk exposure for each individual asset and a portfolio of assets

Reporting dimensions

Business divisions	Business processes	Asset classes	Individual assets and stacks	Legal entities	Regions and countries	Buildings

Exhibit 2 presents the "path to green": the risk-mitigation initiatives enabled by the mature bottom-up approach that bring risk indicators within the risk appetite.

A high-performing cyberrisk MIS is much more than a reporting tool. It is an integrated decision-support system, creating visibility on all relevant assets—end-user devices, applications, infrastructure, networks, and buildings. It gives decision makers access to detailed information on organizational units, regions, and legal entities. It embodies the principles of good cyberrisk governance, from definition and detection to treatment and measurement.

Implementation of the cyberrisk MIS is as critically important as its design. Even the finest aggregated scorecard or the most granular breakdown of KRIs will be useless if executives do not rely on the output for decision making. This is why a good cyberrisk MIS should be customized, reflecting the specific needs of decision makers at levels one and two of a company's hierarchy.

Catalyzing a cybersecurity transformation

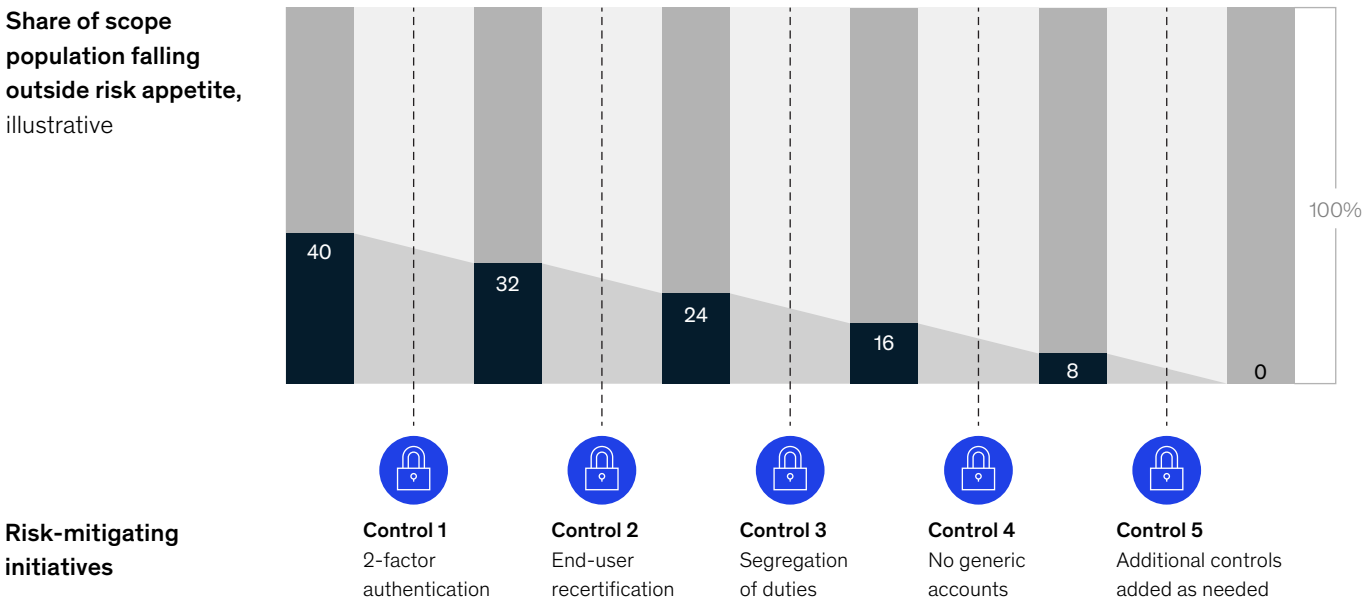
The cyberrisk MIS can catalyze a comprehensive cybersecurity transformation. This happens in the MIS implementation, which in itself is an opportunity to transform the ways companies gather information about cyberrisk and make decisions about countermeasures.

The description of a successful cyberrisk MIS implementation is remarkably congruent with that of a cybersecurity transformation. The steps are as follows:

— Define the scope and objectives. Leaders work up front to define objectives and deliverables. They begin by taking stock of how cyberrisk information is gathered and how executives decide on countermeasures. Cybersecurity governance and organization should be established across the whole company, with common standards and best-in-class reporting for systematic risk identification and prioritization.

Exhibit 2

Risk-mitigation initiatives indicated by the bottom-up aggregation approach provide the 'path to green.'



> **"We don't want to reinvent the wheel. We need a cyberrisk management information system that has a user-friendly interface. It should integrate the best, most recent data from our own sources. It has to be a lean machine. At the same time, it should give us more transparency than we have today."**
>
> **—Financial-services chief information-security officer**

— Avoid patchwork solutions. The cyberrisk MIS must not be regarded as another patch. It should be comprehensive and more accessible than the previous assemblage of stand-alone reports. A good cyberrisk MIS can accommodate different degrees of maturity in different business units. For example, a module can be included that enables managers to upload static reports until dynamic data become available for automatic updates. Generally, the MIS should supply decision makers with the most pertinent information available at any given time.

— Enhance consistency. With improved transparency comes improved consistency. As the transformation proceeds, executives should calibrate their understanding of cyberrisk and cybersecurity. They should ask, "As an institution, how much risk are we willing to accept? What are our biggest threats? What level of protection renders a given asset safe?" Even a seemingly trivial risk topic can initiate fruitful discussions. For example, in defining cyberrisk-warning thresholds, executives can arrive at a common understanding of risk appetite, asset relevance, regulatory requirements, and the return on investments in cybersecurity.

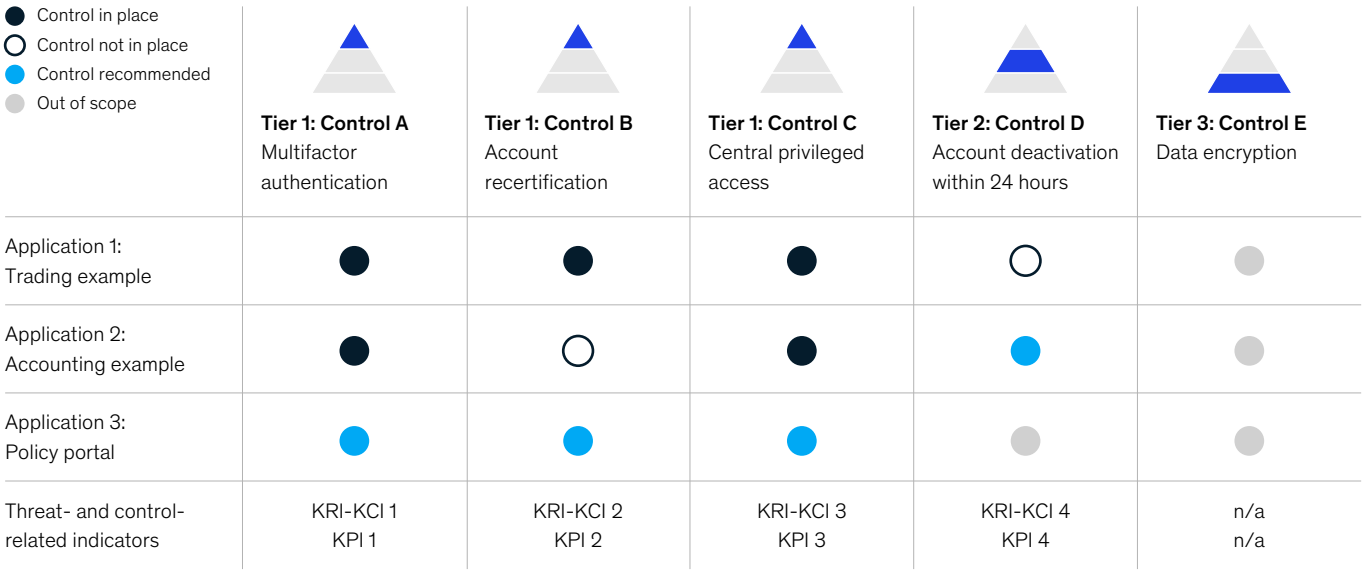
— Shift to a risk-based approach. One of the most powerful benefits of a good cyberrisk MIS is the risk-based approach to controls (Exhibit 3), which replaces the undifferentiated "all controls for all assets" approach. The risk-based approach focuses on the most important assets and the biggest, most probable threats. Decision makers can then allocate investments accordingly. Resilience is thereby improved without an increased cybersecurity budget. In many cases, a state-of-the-art cyberrisk MIS allows reductions in operating expenditure as well.

One company used the fact base it created in implementing its cyberrisk MIS to introduce a tiered

Exhibit 3

The cybersecurity transformation enabled through a cyberrisk management information system includes more effective, less costly differentiated controls.

Cyberrisk management information system, example



Effective information-security risk management is based on asset-centric indicators, including key risk indicators (KRIs), key compliance indicators (KCIs), and key performance indicators (KPIs), revealing compliance issues as well as current and forecasted residual risk exposure.

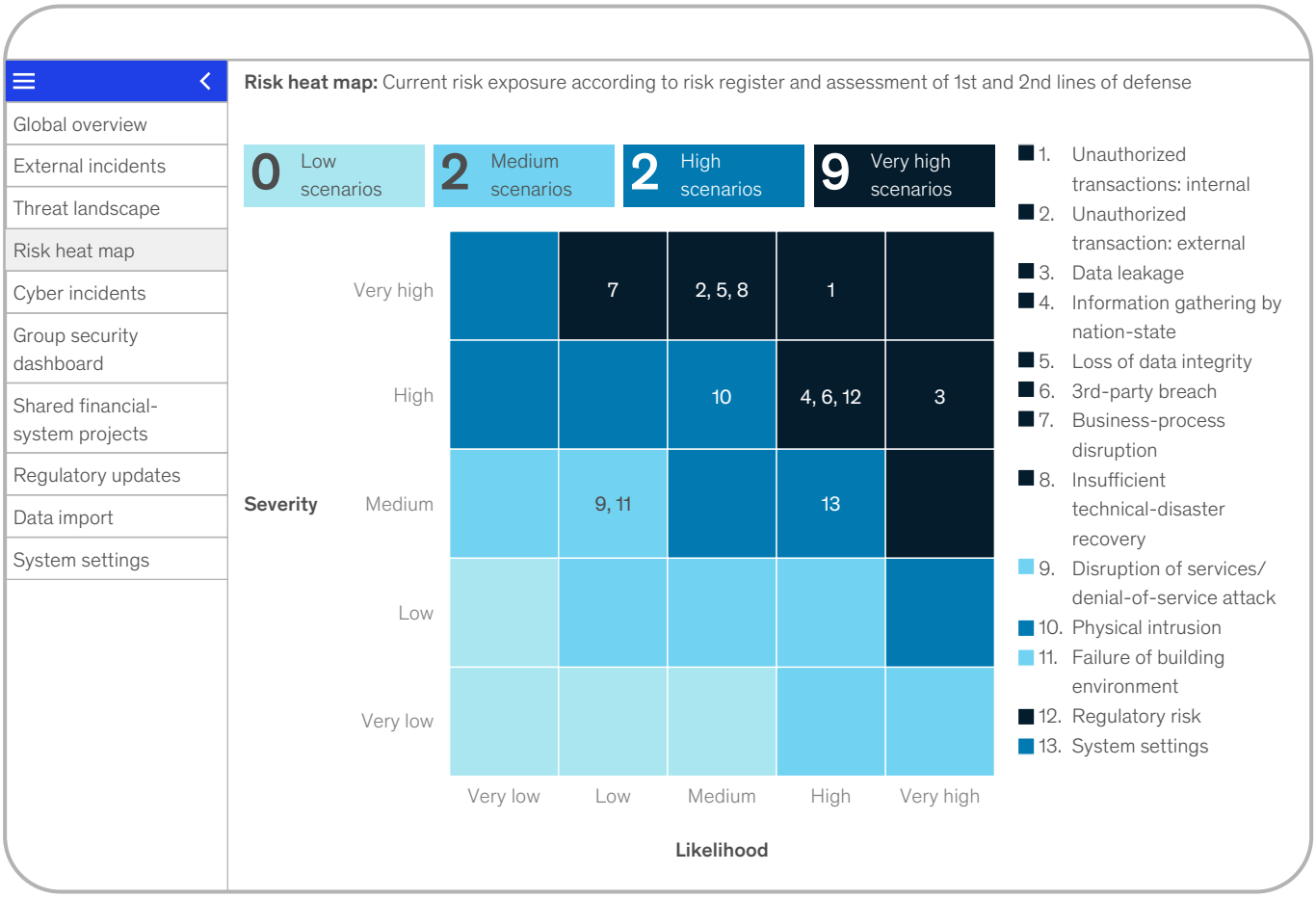
control regime. The company subjected only its most critical, most vulnerable assets (class one) to the full arsenal of controls—from multifactor user authentication to deleting, after 24 hours, the accounts of anyone who left the company. By contrast, it applied only basic controls to the least critical assets (Exhibit 3). As a result of this tiered approach, the company was able to improve compliance with relevant regulatory requirements while reducing the residual risk level. At the same time, it also reduced costs: both direct costs (such as for software licenses) and indirect costs (such as those incurred through the use of cumbersome, undifferentiated controls, even those for low-level applications).

With the right approach, a cyberrisk MIS cybersecurity transformation will provide board-level executives with a concise and easily digestible overview of top cyberrisks. Exhibit 4 shows an MIS cyberrisk dashboard, with the risk heat-map tab open. Other tabs provide the chief risk officer and the chief information officer with the KRIs, KPIs, controls, and progress reports for different functions, organizational levels, and applications. The transformation will foster the use of a common language and a fact-based approach to cyberrisk across the entire institution. Over time, the institution will accrue the benefits of greater cyberrisk transparency, improved cybersecurity efficiency, and greater cyberresilience.

Exhibit 4

The cyberrisk dashboard includes a risk heat map.

Cyberrisk dashboard, example



The fast track to impact

The modular design of the recommended cyberrisk MIS makes it possible to implement a viable version in parts over a period of three to six months, depending on an organization's needs and complexity. For many companies, the most important components—the underlying data structure, the analytical backbone, and the visualization interface—are already in place. In all likelihood, the initial version of a next-generation cyberrisk MIS will not be fully customized to the needs of a given company, but it will be a real working product, not a dummy.

The implementation journey begins with a project team, experts, risk managers, data owners, IT, and other stakeholders jointly determining specific requirements, relevant processes, and data availability. In the building stage, live trial sessions are held to give executives a chance to provide

> “Step by step, we made the cyberrisk MIS our own. The whole process took less than half a year, and yet the finished product really feels like something that was made for us, not like an off-the-shelf solution.”
>
> —Cyberrisk MIS user

feedback on MIS utility. After needed adjustments, the scope is widened and the system is deployed to the entire organization.

Leading institutions that have implemented state-of-the-art cyberrisk management information systems have seen significant improvement in the efficacy of cyberrisk detection and remediation. The platform links operational data with groupwide enterprise-risk-management information accurately and consistently. These cyberrisk systems can become the basis for a comprehensive cybersecurity transformation and part of a holistic risk-based approach to cybersecurity, reducing risk, raising resilience, and controlling costs.

Jim Boehm is an associate partner in McKinsey’s New York office, where **James M. Kaplan** is a partner; **Peter Merrath** is an associate partner in the Frankfurt office, where **Tobias Stähle** is a senior expert; and **Thomas Poppensieker** is a senior partner in the Munich office.

The authors wish to thank Rolf Riemenschnitter for his contributions to this article.