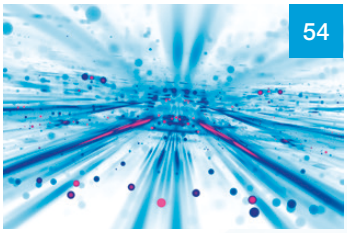
McKinsey&Company

McKinsey on Risk

Highlights

Cybersecurity and the risk function



The advanced-analytics solution for monitoring conduct risk

The lending revolution: How digital credit is changing banks from the inside

Number 6, November 2018

McKinsey on Risk is written by risk experts and practitioners in McKinsey's Global Risk Practice. This publication offers readers insights into value-creating strategies and the translation of those strategies into company performance.

This issue is available online at McKinsey.com. Comments and requests for copies or for permissions to republish an article can be sent via email to Risk@McKinsey.com

Cover image:
© saemilee/Getty Images

Table of contents

Introduction

We are delighted to introduce our latest issue of *McKinsey on Risk*, the journal offering McKinsey's global perspective and strategic thinking on risk. This publication focuses on the risk areas that affect the performance of the world's leading companies, taking a truly global view across business sectors and functions. Articles present deep industry insight and recount hands-on experience to highlight the strategic skills and analytical tools companies are using to transform all areas of risk management.

Our offering begins with a collection of pieces on cyber risk, now a strategic priority in a business environment that has been profoundly reshaped by digitization. Many companies nonetheless continue to treat cybersecurity as a technological or compliance issue, despite years of headline-grabbing systems breaches. In recognition of this misalignment, our lead article demonstrates why security strategy must rest upon a close partnership of the organization's IT, cyber, and risk leaders. A following discussion explains how to build comprehensive dashboards that accurately identify, size, and prioritize cyberthreats for treatment. The section continues with a piece on cyberthreats posed by company insiders, whether employees or contractors, and concludes with a consideration of government's role on the cyber risk terrain.

This issue then continues with an exploration of the latest thinking on how nonfinancial institutions should approach risk management. We conclude with articles describing the contours of the digitally transformed credit journey and the ways in which advanced analytics is being used to monitor conduct risk.

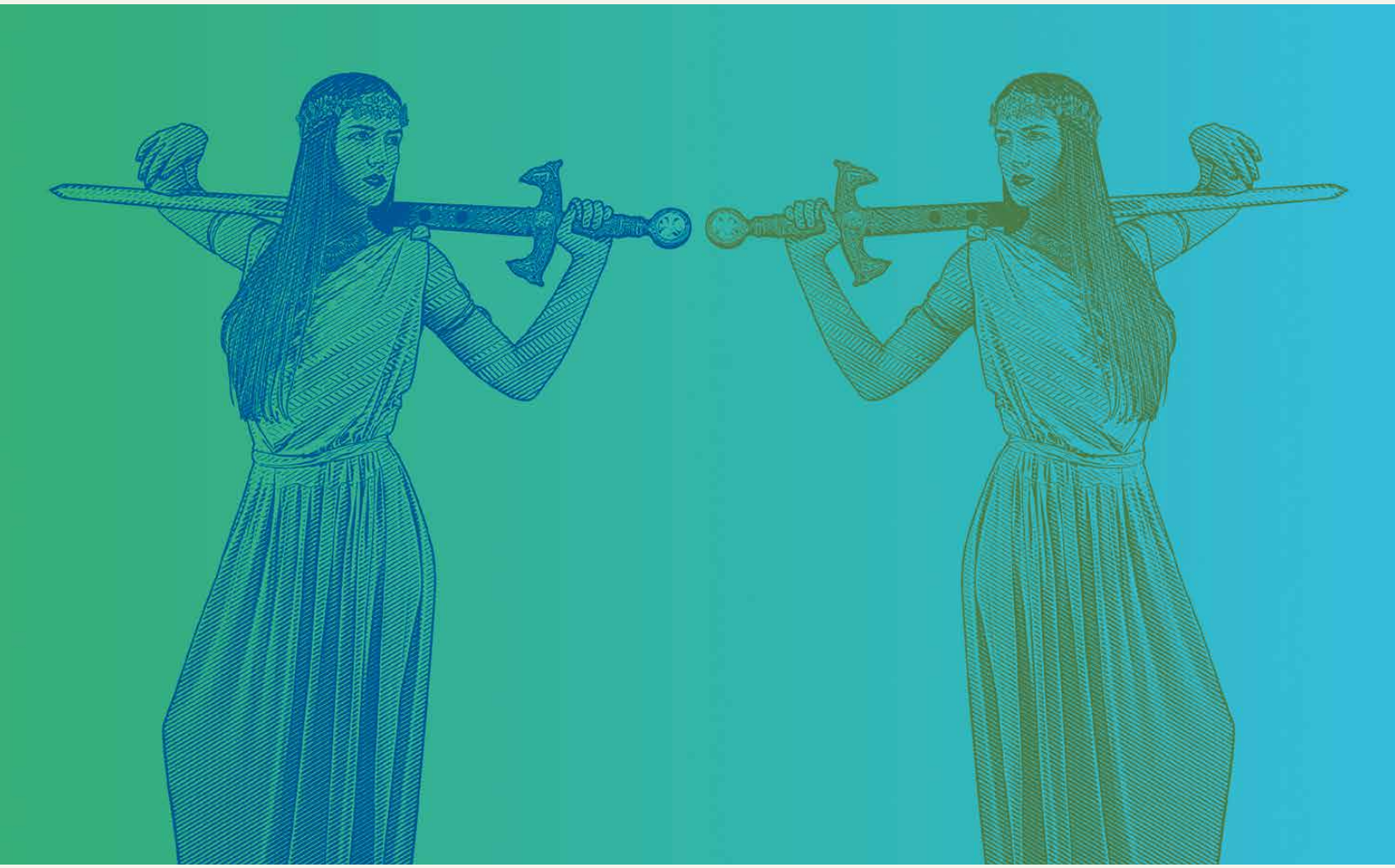
We hope you enjoy these articles and find in them ideas worthy of application. Let us know what you think at Risk@McKinsey.com and on the McKinsey Insights app.

Thomas Poppensieker
Chair, Global Risk Editorial Board

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



Most CEOs of large organizations are convinced of the existential dimensions of cyber risk. 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 among these teams is the optimal approach, as 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 will it 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, it is often sidelined in the area of cyber risk. 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 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 according to priority.

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 work flow. 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 cyber risk as well. The question is, how best to integrate risk into the cybersecurity environment?

Barriers to CISO–Risk collaboration

While organizational models for handling cyber risk 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 cyber risk, 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 cyber risks.

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. This relationship benefits both the first and second lines. The first line becomes more aware of how cyber risk 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 cyber risks, 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, the 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 cyber risk 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 cyber risk 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 cyber risk. 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 cyber risk 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 cyber risk 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 cyber risks 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 cyber investment 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 cyber risk 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 cyber risk reporting, so that cyber risk 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 work flow 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 the 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 will 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 process 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 cyber risk 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 work flows 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.

An essential purpose of the model is to ensure that the CRO and the risk group understand cyber risk 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 cyber risk 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 cyber risk, sets the agenda for cyber investments, 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's 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 cyber risk agenda on an enterprise-wide basis.

- The 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 cyber risk 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 cyber risks, 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 nontechnical 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 it insight into enterprise risks and gain its buy-in to cyber risk 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 cyber risk 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.

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 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 cyber risks.

■ ■ ■

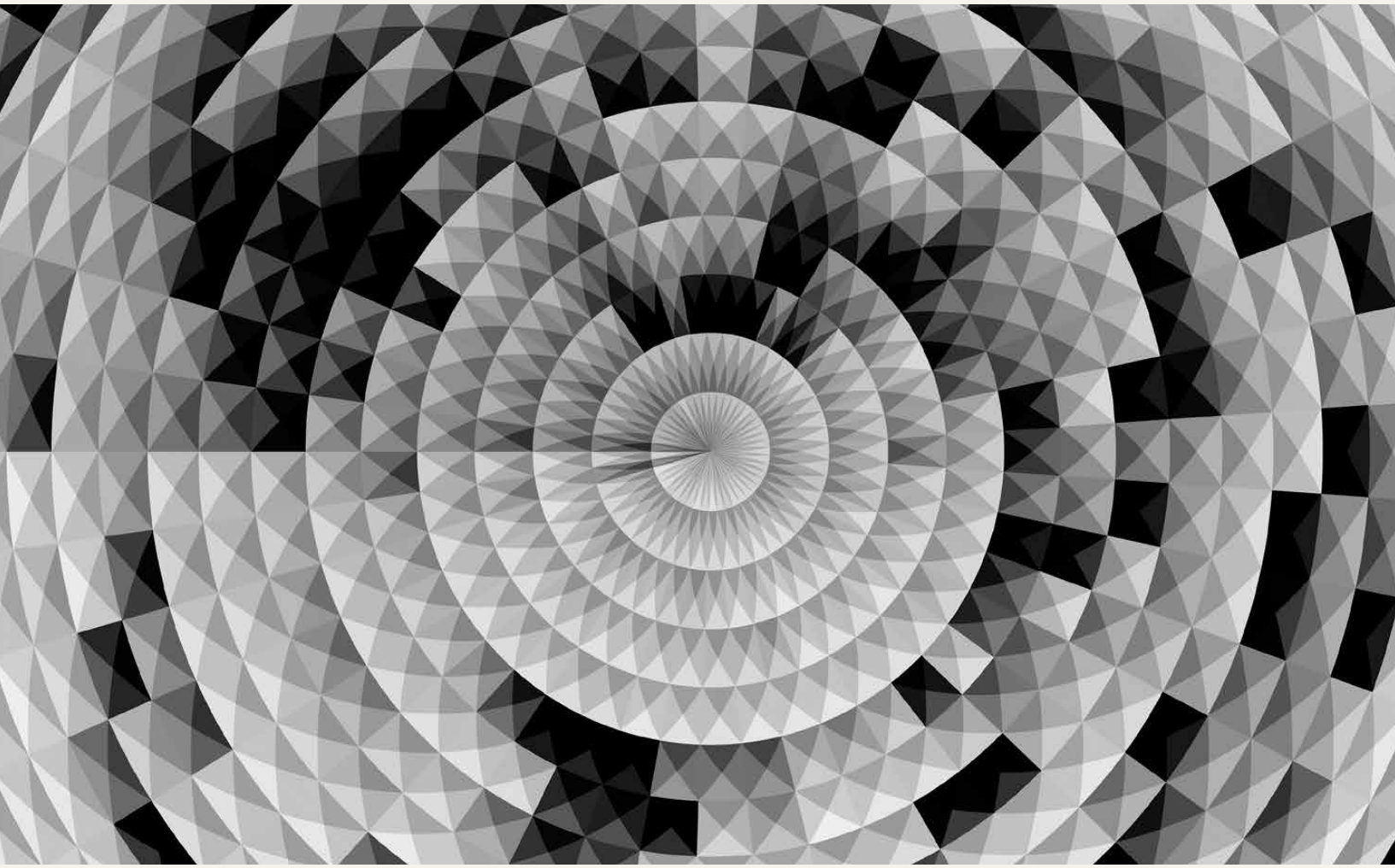
With cyberthreats mounting in number and sophistication, large institutions can no longer protect against all risks equally. The threats posing the most danger to the business must be identified and neutralized first. For this to happen, the risk function must be deeply embedded in cybersecurity planning 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 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.

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



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

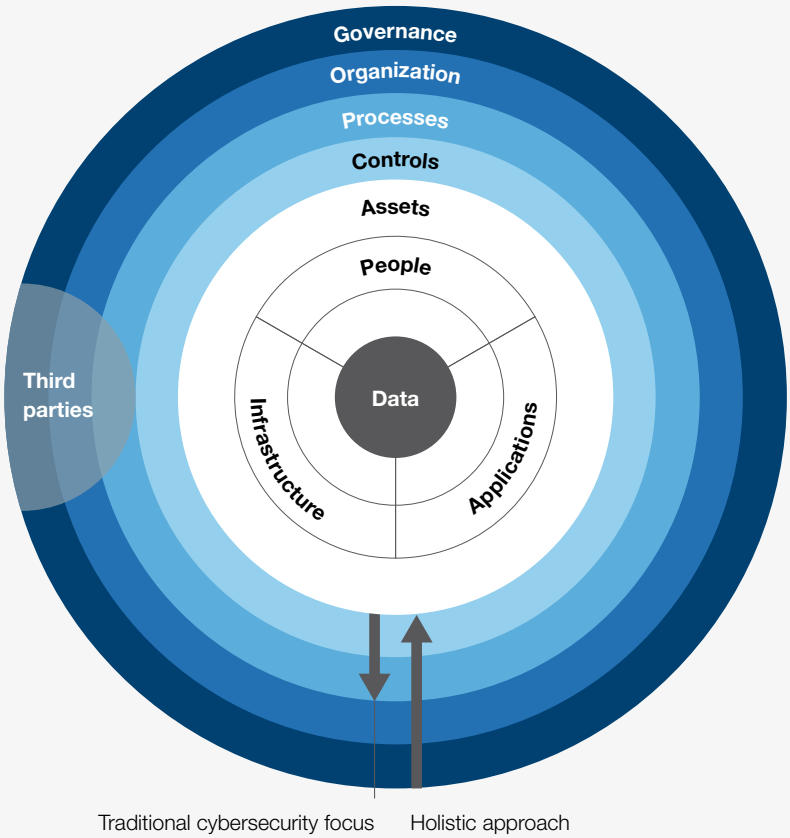
A holistic approach to cybersecurity can address these failings and their implications for governance, organizational structures, and processes (Exhibit 1).

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

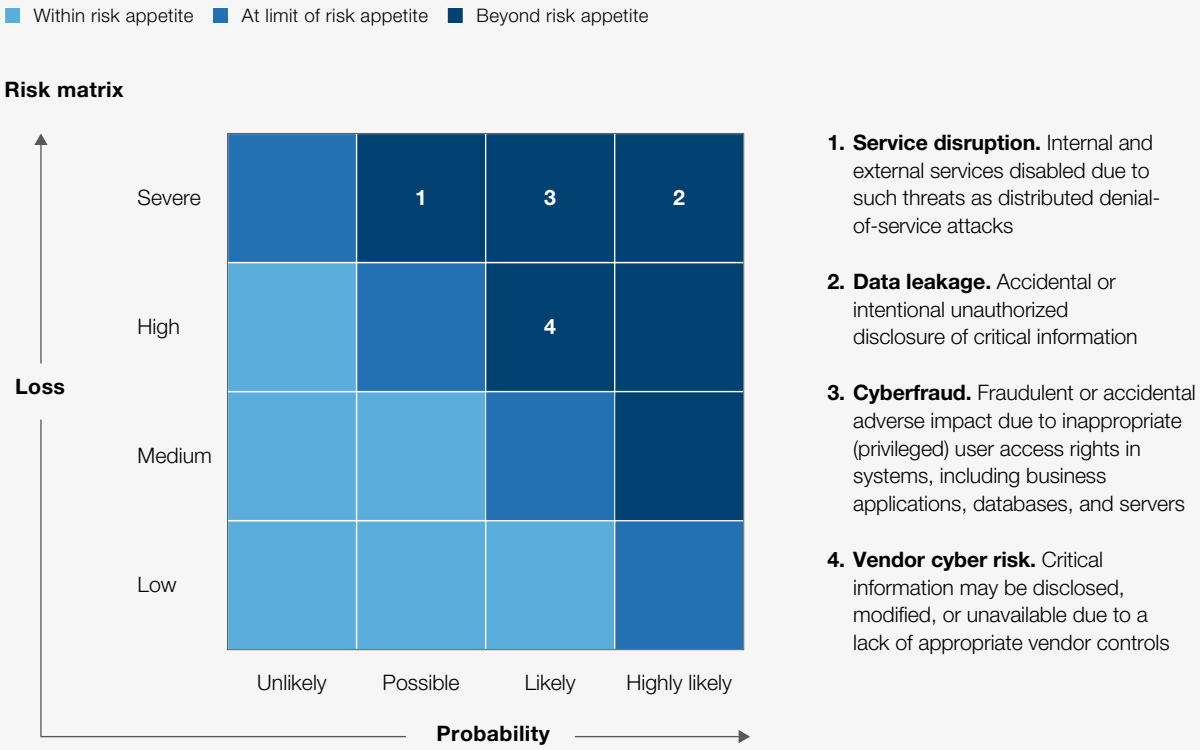
Exhibit 2 **The holistic approach lays out a path to root-cause mitigation of top risks in four phases.**

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

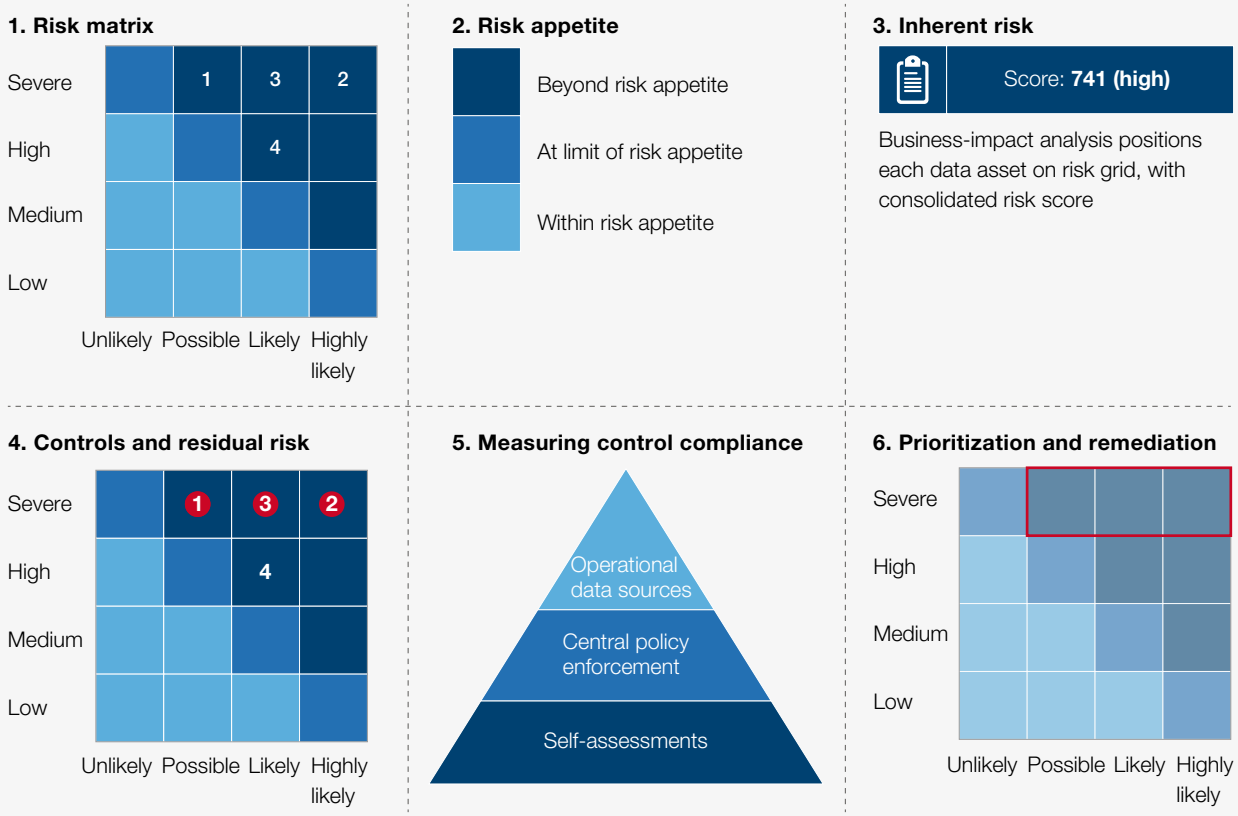
Leading companies include progress updates in their cyber risk reporting. The updates provide information on the status of counter-risk initiatives and

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

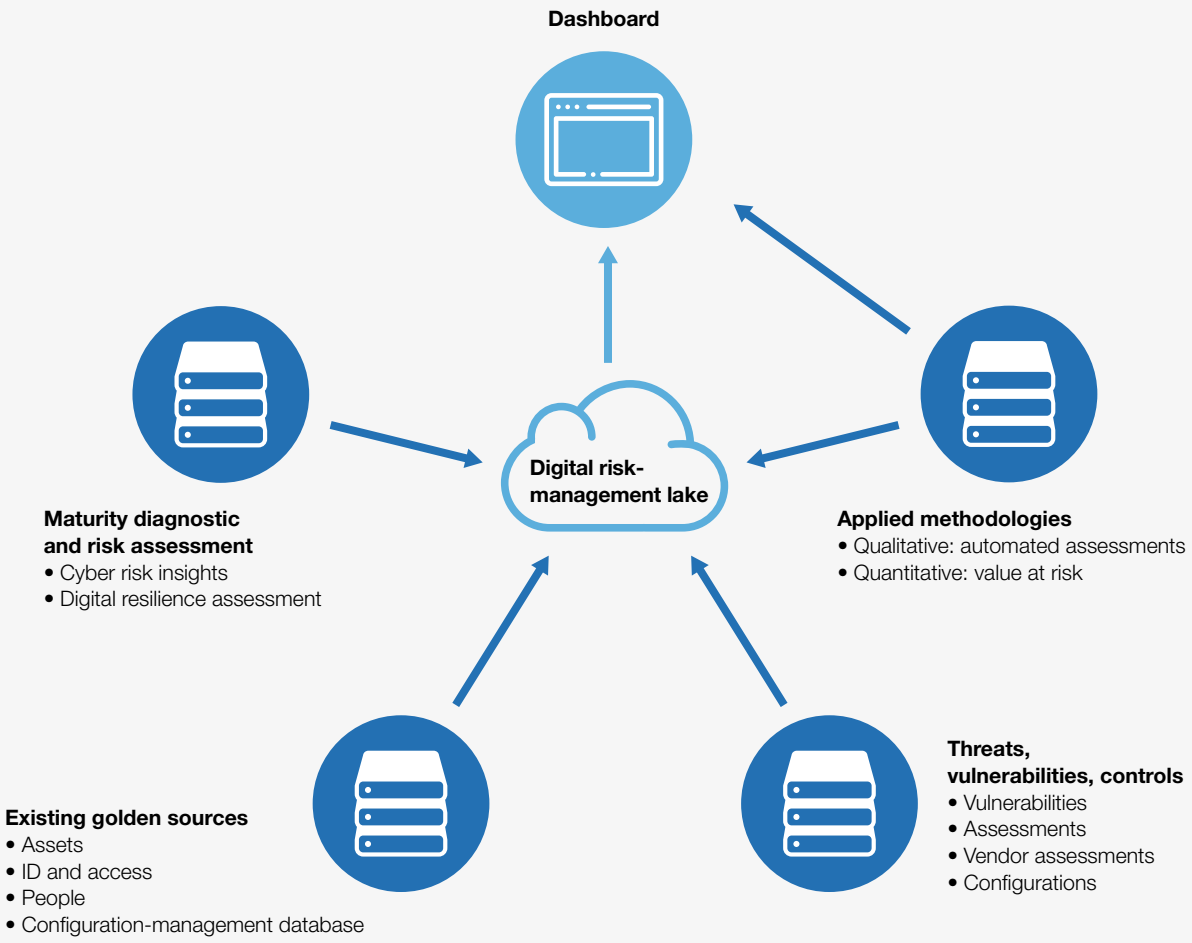
A good cyber risk dashboard is one designed to promote good decision making. One way it does this is by simplifying details, intricate KRIs, and complicated visuals to communicate the most essential information—an essentially complete risk profile. An executive in the financial-services industry explained 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; and **Thomas Poppensieker** is a senior partner in the Munich office.

Insider threat: The human element of cyber risk

Cyber programs often miss the significant portion of risk generated by employees, and current tools are blunt instruments. A new method can yield better results.

Tucker Bailey, Brian Kolo, Karthik Rajagopalan, and David Ware

Insider threat via a company's own employees (and contractors and vendors) is one of the largest unsolved issues in cybersecurity. It's present in 50 percent of breaches reported in a recent study. Companies are certainly aware of the problem, but they rarely dedicate the resources or executive attention required to solve it. Most prevention programs fall short either by focusing exclusively on monitoring behavior or by failing to consider cultural and privacy norms.

Some leading companies are now testing a microsegmentation approach that can target potential problems more precisely. Others are adopting in-depth cultural change and predictive analytics. These new approaches can yield more accurate results than traditional monitoring and can also help companies navigate the tricky business of safeguarding assets while also respecting employees' rights.

Understanding the threat

Organizations sometimes struggle to clearly define insider threat. In this article, we use the term to mean the cyber risk posed to an organization due to the behavior of its employees, rather than other kinds of insider threat, such as harassment, workplace violence, or misconduct. For these purposes, contractors and vendors are also considered employees; many of the largest cases in recent memory have trusted third parties at their center.

Insider threats arise from two kinds of employees: those who are negligent and those with malicious intent (see sidebar, "Double trouble"). Negligent or co-opted insiders are easy for companies to understand; through poor training, middling morale, or pure carelessness, usually reliable workers can expose the company to external risks. However, organizations often misunderstand malicious insiders in two ways.

Double trouble

Two types of workers can create cyber risk:

Malicious insiders are those who purposefully seek to benefit themselves at the organization's expense or to harm the organization directly. They might steal valuable data, commit fraud for financial gain, publicly expose sensitive information to attract attention, or sabotage IT systems in disgruntlement. Most organizations focus their attention on malicious insiders, using activity-monitoring software and small investigative teams.

Negligent or error-prone insiders may not harm an organization intentionally but expose the organization to risk through their mistakes or carelessness. This can happen in two ways. First, an employee can carelessly create a vulnerability, which can be exploited by attackers directly. For example, a developer might misconfigure a company's Simple Storage Service (S3) buckets, or someone might lose a hard drive carrying sensitive data. Employees can also make themselves personally vulnerable to attack and co-option. For example, by sharing too much personal information online, employees may make themselves easy targets for spear-phishing attacks, in which attackers co-opt a user's account and use it to conduct further nefarious activities.

First, malicious insiders do not always seek to harm the organization. Often, they are motivated by self-interest. For example, an employee might use client information to commit fraud or identity theft, but the motive is self-enrichment rather than harm to the employer. In other cases, employees may be seeking attention, or have a "hero complex" that leads them to divulge confidential information. They might even think they are acting for the public good, but in reality they are acting for their own benefit. Understanding motive can help companies shape their mitigation strategy.

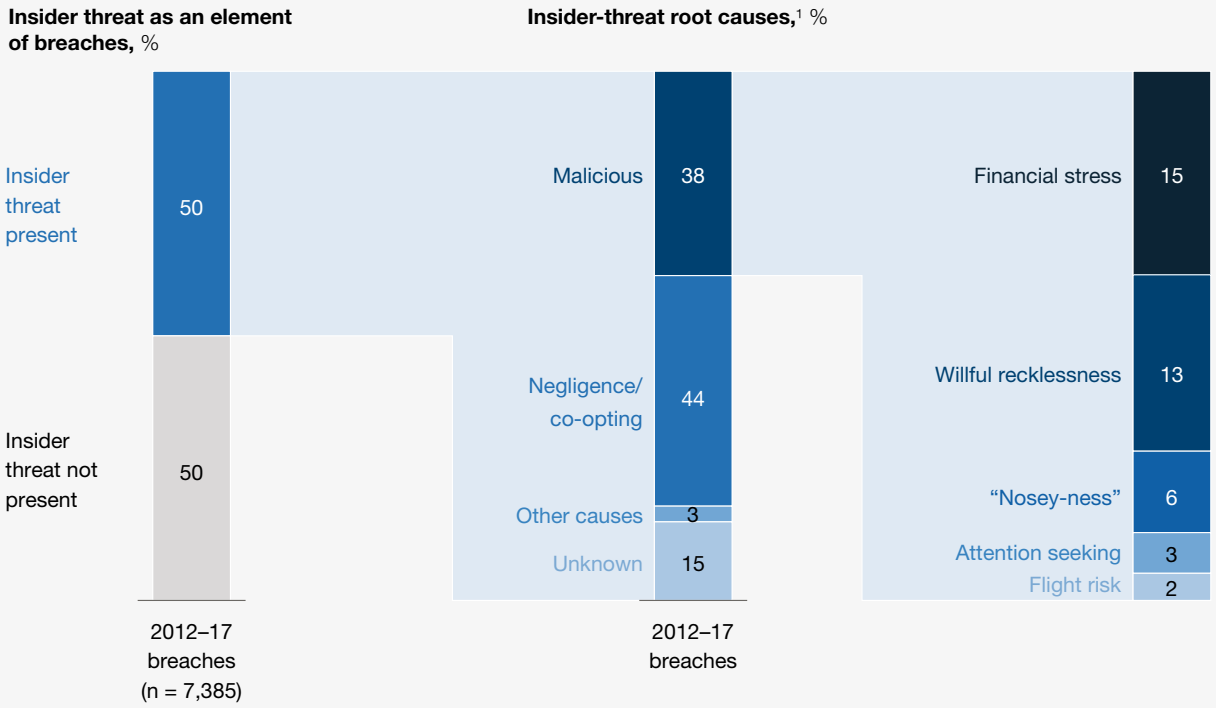
Second, malicious insiders rarely develop overnight or join the company intending to do it harm. In most recent examples of malicious insider events, normal employees became malicious insiders gradually, with months or years of warning signs leading up to a culminating insider event.

How big an issue is it, really?

In a world of competing cyber priorities, where needs always seem to outpace budgets, it can be tempting to underinvest in combating insider threat. The risk is not well understood, and the solution feels less tangible than in other cyber areas. Many executives have asked us, "Is this actually an important issue? How much risk does it represent?"

We recently reviewed the VERIS Community Database, which contains about 7,800 publicly reported cyberbreaches from 2012 to 2017, to identify the prevalence of insider threat as a core element of cyberattacks. We found that 50 percent

Exhibit 1 **Insider threat is present in 50 percent of cyberbreaches.**



[1] Figures are approximate and may not sum, because of rounding.

Source: VERIS Community Database

of the breaches we studied had a substantial insider component (Exhibit 1). What's more, it was not mostly malicious behavior, the focus of so many companies' mitigation efforts. Negligence and co-opting accounted for 44 percent of insider-related breaches, making these issues all the more important.

In addition to being frequent, insider-threat breaches often create substantial damage. We have seen high-value events in which customer information was stolen through negligence and by malicious insiders in financial services, healthcare, retail, and telecom in recent years. Some companies lost hundreds of millions of dollars. Pharmaceutical and medical-products companies, as well as governments, have seen a significant rise in intellectual-property theft by malicious insiders.

Why current solutions fall short

To combat the risks of malicious insiders, most companies rely on user-behavior monitoring software (Exhibit 2). These rules-based or machine-learning-based applications ingest troves of data about employee actions, especially their use of IT systems. Generally, they attempt to identify divergence from what is considered "normal" behavior for that employee. When the software spots an anomaly, a small team investigates.

While this method can be helpful, we find that it usually falls short, for four reasons:

- By the time negative behaviors are detected, the breach has often already occurred. The

Exhibit 2 **Current methods of insider-threat management fall short.**

Typical approach	Prevention and monitoring	Event detection: Behavior-variability analysis	Investigation	HR/business-unit action
	• "Dragnet" monitoring of all employee actions, all the time • General controls and preventions	• Analyze divergence from "normal" behavior	• Manually investigate numerous cases	• Take actions on a case-by-case basis
Pain points/risks	• Massive number of signals • High risk of misuse of data • Perception of privacy invasion • Preventions not customized to risks, actors, and actions	• Bad behaviors can be built into baseline • Huge volume of false positives (>30% in some cases)	• Often a long backlog of cases • Little ability to prioritize investigations	• Uncertainty about how to manage between investigation and action • Actions not well defined or tailored to individual incidents

organization is already at a disadvantage, and it cannot deploy an active defense.

- Monitoring for "divergence from normal behavior" creates a huge number of false positives, wasting much of the investigation team's time.
- Serial bad actors may not be caught; malicious activity may be built into the baseline of "normal" activity.
- Collecting massive amounts of employee data creates privacy concerns and significant potential for abuse.

Beyond these issues, some organizations take this type of monitoring to an extreme, deploying military-grade software and conducting full-blown intelligence operations against their employees. Several recent news stories have highlighted the risks of overstepping the organization's cultural and privacy norms. Best practices and necessary precautions in the defense industry may be seen as invasive at a bank or insurer.

Finally, to the extent that companies pursue insider threat, they often focus on malicious actors. While most cyber organizations know that negligence is an issue, many start and end their prevention efforts with half-hearted employee education and anti-phishing campaigns.

A better way

Some leading cybersecurity teams are using a different approach, built on three pillars:

- *Microsegmentation* allows the organization to home in on the "hot spots" of risk and take a targeted rather than blanket approach to threat monitoring and mitigation.
- *Culture change* makes malicious, co-opted, or negligent risk events less likely, and puts the company in a preventive rather than reactive posture.
- *Prediction* allows an organization to identify and disrupt insider activities much earlier in the threat life cycle.

Microsegmentation

Rather than going immediately to wholesale monitoring, we believe that organizations should take a much more nuanced approach, tailored to their information assets, potential risk impact, and workforce. The key to this approach is microsegmentation, which identifies particular groups of employees that are capable of doing the most damage and then develops focused interventions specific to those groups.

To create a microsegmentation program, the first step is to understand the business capabilities or information most important to protect. Next, companies can use identity-and-access-management (IAM) records, as well as organizational and HR information, to determine which groups and individual employees have access to those assets. These groups form the microsegments that are most important for the program to focus on. For each segment, a company can then determine which types of insider threats are most likely to cause damage, and it can create differentiated strategies to monitor and mitigate insider events.

Imagine that a pharmaceutical company wants to protect the intellectual property (IP) created in new-drug development. An analysis of IAM and HR data reveals that specific portions of its product-development and its R&D organizations represent the highest risk. The company knows that sabotage

of this kind of IP is relatively rare (other researchers would easily catch mistakes), but that flight risks—scientists who take IP with them when hired by competitors—are very probable. The company designs strategies to identify flight risks in the R&D team (such as people who missed promotions, poor workforce satisfaction, and low pay relative to peers), and then monitors the group for these characteristics. The company could then design interventions, such as retention programs, specifically for its flight risks.

Microsegmentation offers three key benefits. First, it creates a clearer understanding of risk; not all insider-threat events are created equal. Second, it allows organizations to identify a clear set of remediation actions, tailored to a particular group of employees. This helps them to move from reacting to insider-threat events to preventing them. Finally, the analysis allows the organization to monitor groups rather than individuals, using metrics such as employee attrition and the workforce satisfaction of a team rather than individual behaviors. This provides significant privacy benefits.

Exhibit 3 shows an illustrative microsegmentation analysis for several kinds of information assets.

Exhibit 3 **Microsegmentation can reveal groups at risk, the actions they might commit, and their likely personas.**

Threat assessment, illustrative example

■ Very likely ■ Somewhat likely ■ Not likely

Top assets	Employee populations with access	Insider-threat actions they might take			Likely personas involved
		Fraud/theft	Exposure	Destruction	
Intellectual property for new products	• R&D team • Business-unit (BU) exec	■		■	• Flight risk • Disgruntled
Financial forecasts	• Finance/investor-relations team • BU execs	■	■		• Financially stressed • Negligent
PII/PHI[1]	• HR team • Sales team	■	■	■	• Negligent • Reckless • Snooper
High-net-worth customer information	• High-net-worth sales and delivery team	■		■	• Flight risk • Financially stressed
Core financial platform	• IT team • BU execs	■		■	• Saboteur • Disgruntled
Records of corporate conduct	• HR/legal		■	■	• Attention seeker

[1] PII = personally identifiable information, PHI = protected health information.

Culture change

While many programs focus on catching and responding to negative behaviors, it is also vitally important to directly and assertively address the cultural issues that drive negligence and malicious behavior.

To combat negligence and co-opting, companies often conduct rudimentary cybersecurity training, as well as phishing testing. Too often these focus only on behavior—educating employees on proper cyber procedures—and miss the attitudes-and-beliefs part of the equation. Targeted interventions (such as periodic communications on cyber impact) help employees see and feel the importance of "cyber-hygiene," and purposeful reinforcement from senior executives is critical to achieving workforce buy-in. Best-in-class organizations rigorously measure both behaviors and attitudes and develop comprehensive change plans to beat cyber-negligence, complete with targets and clear owners within the organization.

Addressing the drivers of malicious behavior is an even more personal task. The drivers vary for each organization, and often for each microsegment. For instance, they might include personal financial stress, disgruntlement over lack of promotion, or flight risk due to poor management. Organizations that successfully address drivers of malicious behavior often begin by analyzing workforce trends (using satisfaction surveys, for example) to determine potential hot spots. They then design changes in process, governance, hiring, compensation, and so on, specific to the identified risk areas aligned to their microsegmentation strategy. For example, if an employee group has a high prevalence of "flight risks" due to disgruntlement over a manager, the organization may require leadership coaching or even rotating the manager out of the group. If financial stress seems to be an issue, the organization may choose to provide free financial-planning help or to reevaluate its compensation model.

Prediction

Advanced organizations are taking one further step to identify groups or individuals early in the threat life cycle: predictive insider-persona analytics. The main personas that present a risk are well established and have been studied at length. High-performing organizations have identified the markers of these personas and actively monitor these markers for specific personas, rather than looking for divergence from normal. This analysis can identify a group or individual likely to represent a threat well before the event takes place; companies can then take steps to mitigate the threat. Exhibit 4 outlines the predictive analysis for identifying disgruntled employees, one of the established personas.

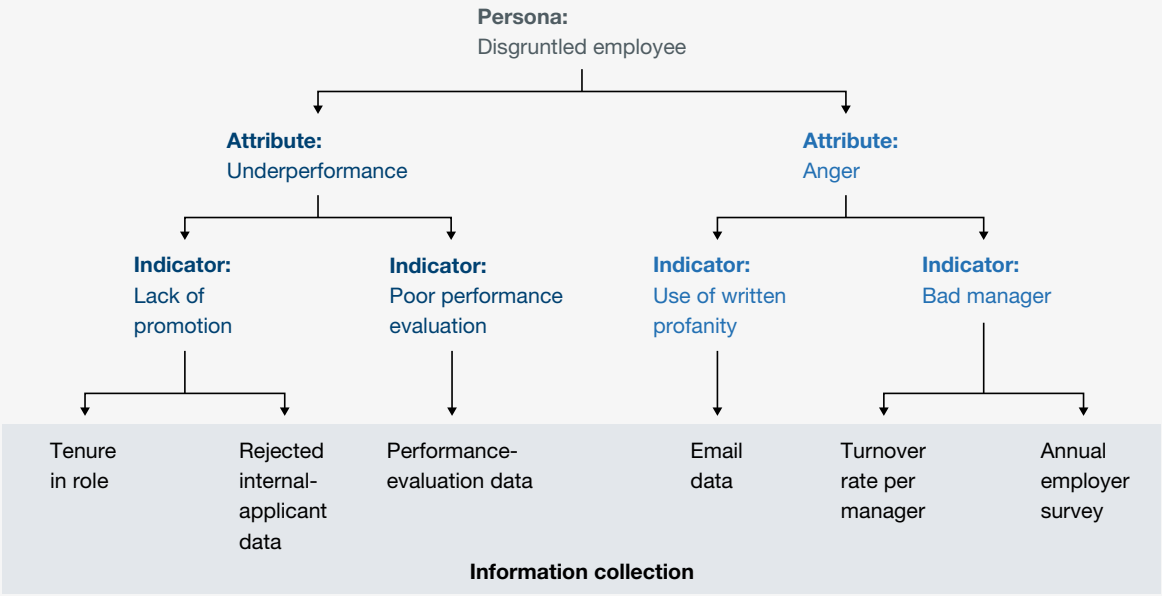
While powerful, these analytics require careful consideration about their use in the context of an organization's culture, its privacy norms, and the evolving standards of privacy in society at large. Failing to think it through often results in employee complaints about invasion of privacy.

A few words on privacy

Privacy is an inherently personal and intangible subject—its meaning and importance varies by geography, by industry, by company, and often by individual. Many individuals are fiercely protective of their privacy, even when at work and even in their use of corporate assets. This is never more true than when it comes to monitoring their use of communications systems such as email—even corporate email. As standards on individual and corporate privacy rights evolve (for example, through the European Union's General Data Protection Regulation), organizations need to design their

Exhibit 4 **The markers of risky personas can give companies a head start on intervention.**

Example risky persona



insider-threat programs based on what will work within their own cultural and regulatory environments. In all cases, organizations need to tailor their insider-threat program by respecting what data may be gathered, how they may be collected and used lawfully, and how best to create awareness of the program, both generally and specifically, with potentially affected staff.

While each organization must make its own trade-offs between privacy and risk, we believe our approach will make such trade-offs easier to navigate than traditional programs. First, the microsegmentation approach does not require a baseline of individual activity (by which traditional programs judge "normalcy"), which some organizations could perceive as a privacy concern. Second, microsegmentation presents natural groups of employees for analysis, which improves the anonymity of the analysis. Microsegmented groups can be analyzed for potential threats with reasonable precision of results. Investigations of specific individuals can be conducted only when there is reasonable suspicion of a threat and must be done in line with applicable law.

■ ■ ■

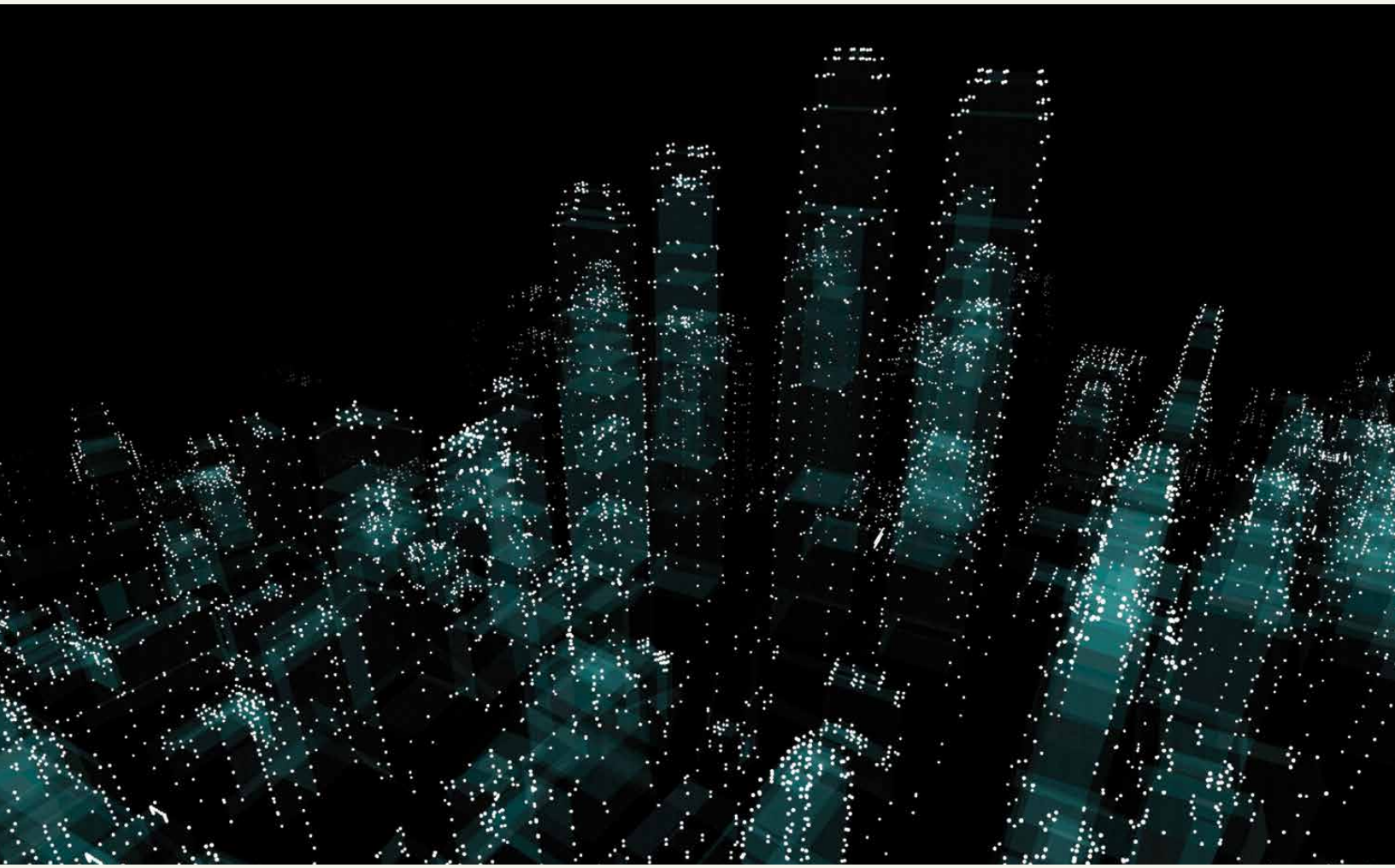
Insider threat is one of the largest problems in cybersecurity, representing a massive share of attacks and financial damages. Monitoring technologies have their place in organizations' cyber arsenal. But their effectiveness increases significantly when combined with more nuanced approaches, like microsegmentation, prediction, and direct cultural engagement. ■

Tucker Bailey is a partner in McKinsey's Washington, DC, office, where **Brian Kolo** is a digital expert and **David Ware** is an associate partner; **Karthik Rajagopalan** is a consultant in the Dallas office.

Asking the right questions to define government's role in cybersecurity

There is no one-size-fits-all approach for governments to manage cybersecurity. But asking some key questions can help leaders get started.

Mary Calam, David Chinn, Jonathan Fantini Porter, and John Noble



Government leaders are increasingly aware that promoting prosperity and protecting national security includes providing cybersecurity. That means demonstrating that a nation, state, region, or city is a safe place to live and do business online. And it includes deterring cyberattacks, preventing cyber-related crime, and protecting critical national infrastructure while also maintaining an environment that makes technological progress easy.

It is a tall order. National security and criminality are different—and multifaceted—in the digital arena. Tools developed by governments to provide security are seized, weaponized, and proliferated by criminals as soon as they are released. Malware-development utilities are available on the dark web, enabling criminal activity even by those with only basic digital skills. Cyberthreats cross national boundaries, with victims in one jurisdiction and perpetrators in another—often among nations that don't agree on a common philosophy of governing the internet. And complicating it all, criminal offences vary, legal assistance arrangements are too slow, and operating models for day-to-day policing are optimized for crimes committed by local offenders.[1] Even relatively low-level threats can have impact on a vast scale.

Each country is addressing the challenge in its own way, just as companies tackle the issue individually. Approaches vary even among leading countries identified by the Global Cybersecurity Index, an initiative of the United Nations International Telecommunications Union. Differences typically reflect political and legal philosophy, federal or national government structures, and how far government powers are devolved to state or local authorities. They also reflect public awareness and how broadly countries define national security—as well as technical capabilities among policy makers.

Despite such differences, our work with public- and private-sector organizations suggests a series of questions government leaders can ask to assess how prepared they are.

Who is accountable?

An effective national cybersecurity ecosystem crosses traditional institutional boundaries and includes a wide range of departments, agencies, and functions, both military and civilian. Many countries have yet to clarify who is accountable across all dimensions of cybersecurity or to impose a single governance structure. That lack of clarity can result in a confused response to crises and inefficient use of limited resources.

In our experience, a single organization should have overall responsibility for cybersecurity, bringing operational activity and policy together with clear governance arrangements and a single stream of funding. Particularly when responding to a cyberattack, clarity of leadership and decision making is vital to ensure the correct balance among helping victims recover quickly, taking measures to protect others (by increasing resilience and attacking the source of the attack), and performing a criminal investigation of those responsible. While some national and state governments have consolidated accountabilities into a clear structure, such as Estonia's Cyber Security Council, or have well-established and tested crisis-response mechanisms that they have adapted for use in cyberevents, as in Sweden, many others do not.

Key skills are often in short supply. Knowledge of the threat, resources, and authority to make decisions may all sit in different places across government. This reduces operational effectiveness and can also result in weak legislation, bad policy, and lack of investment. Some countries are starting to address these challenges. Germany, for example, has

strengthened its Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security) to lead its national cybersecurity strategy and establish shared cybersecurity services for government.

The United Kingdom's National Cyber Security Centre (NCSC) is also widely cited as a model for government-level cybersecurity. It brings together analysis, assessment, and crisis response to provide advice to critical national infrastructure organizations, businesses more broadly, and the public (exhibit). Its operating model involves both access to highly sensitive intelligence and dissemination of public information. And it brings together cybersecurity experts from government and the private sector in a single body.

Questions governments can ask include the following:

- Are lines of accountability and remits clear—both for policy and for crisis response?
- Is it clear how government priorities are decided and communicated?
- Is there a coherent, cross-government strategy? Is it reviewed and refreshed regularly?
- What performance metrics does the government have for the strategy? How are they monitored?
- What information does the government publish about progress on cybersecurity?
- Do the responsible parts of government come together regularly to agree on plans and review progress?

Exhibit

The National Cyber Security Centre leads the UK government's cybersecurity work.

Responsibilities:

- Protect the UK's critical services from cyberattack.
- Manage major cybersecurity incidents.
- Improve the underlying security of the UK internet through technological improvement and advice to citizens and organizations.

Sample functions:

- Develops knowledge and distills insight on cybersecurity into practical guidance for public consumption.
- Responds to cybersecurity incidents to reduce the harm they cause to people and organizations.
- Applies industry and academic expertise to build capability in the cybersecurity system.
- Secures public- and private-sector networks.
- Provides a single point of contact for government agencies, departments, and organizations of all sizes.
- Collaborates with law-enforcement, defense, intelligence, and security agencies and international partners.

Source: National Cyber Security Centre, ncsc.gov.uk

How centralized should you be?

Some countries have consolidated their audit and regulation functions in a centralized agency. Japan, for example, has its Cyber Security Strategic Headquarters, and Romania has its Association for Information Security Assurance. Others, such as India, have dispersed audit functions across multiple bodies. Both models can work, but as India's *National Information Security Policy and*

Guidelines illustrates, a decentralized model—in this case, ministries are tasked to self-audit and bring in external auditors—requires clear national guidelines and standards. Israel's benchmarking and accreditation arrangements have also been key to raising standards across all sectors.

At the very least, governments can insist on putting the reporting of cyberevents by victims and the sharing of vulnerabilities by suppliers into a single reporting, analysis, assessment, and response hub. In Germany, for example, federal legislators have sought to amend the law to require companies to register any cyberincidents in which they are a victim. Australia introduced a notifiable-data-breaches scheme in 2017, making it a legal requirement to notify affected individuals and the Office of the Australian Information Commissioner of serious data breaches.[2] Ideally, governments will also make it easy for citizens and businesses to report such breaches through an automated platform to facilitate responses, advice, and feedback. Such platforms will also increase transparency around threats and steps to mitigate them.

Sectoral regulators have a more significant role to play in raising cybersecurity standards than has perhaps been recognized. There are moves toward a more regional approach to regulation, reflecting the cross-border digital world: for example, the EU Commission's proposals to develop a regionwide framework of cybersecurity standards.

Questions governments can ask include the following:

- To what extent do data protection and privacy regulations reflect the challenges of the digital age?
- How coherent is the approach to cyber regulation across different sectors of the economy and the wider information-and-communications-technology supply chain? What advice does the government provide?
- Does the criminal law adequately address offenses committed online?
- How closely have policies and regulation been developed in partnership with private-sector operators who will be affected?

How can you work with the private sector?

Governments do not have a monopoly on (or even the largest role in) cybersecurity. Open and trusting relationships with the private sector and academia are essential. Governments need commercial organizations to put more emphasis on cybersecurity, particularly as many companies operate across shared digital platforms. When companies and academic institutions have more knowledge, expertise, and capability, governments can work with them to develop the knowledge and tools needed to strengthen the ecosystem.

Many attacks could be prevented by basic security precautions and maintaining up-to-

Governments need commercial organizations to put more emphasis on cybersecurity, particularly as many companies operate across shared digital platforms.

date patches, yet relatively few countries have invested significantly in education or training programs. One that has is Israel. Its investment in cybersecurity and integration of it into the educational curriculum, its extracurricular activities for high-school students, and its national military service have created a thriving, globally competitive, professional cybersecurity market. The Israeli government has also worked with the private sector, both to build capability and awareness and to grow the economy through the cybersecurity sector—by investing in R&D, for example.

Another example is Singapore, in which the National Cybersecurity R&D Programme supports public–private research partnerships. These are funded by $190 million Singapore dollars ($137.85 million) in the national strategy for developing research and the creation of the National Cybersecurity R&D Laboratory at the National University of Singapore.

And working with industry is also key to the United Kingdom's NCSC, where the sharing of information and expertise includes a unique collaboration between a highly classified intelligence organization and the private sector. Its Cyber Essentials framework is a unified tool for assessing and guiding the development of cybersecurity for private-sector companies. Any company bidding for government contracts must confirm that it is compliant with the scheme. In conjunction with the Centre for the Protection of the National Infrastructure, NCSC also accredits companies under the government's cyberincident-response scheme as providers of technical-mitigation services.

Beyond that, few countries have made efforts to improve cybersecurity in small and medium-size businesses. These are likely to have the least resources and knowledge to build their own cybersecurity. Cybersecurity vulnerabilities in these companies can reduce their own economic value. But they can also be a weak link for bigger firms, creating vulnerabilities as they provide goods and services, including to governments.

Questions governments can ask include the following:

- To what extent does the government sponsor or invest in cybersecurity R&D?
- To what extent does the government support cybersecurity training, education, and awareness raising for businesses, those in work, those in education, and those in the general population?
- Does the government engage the private sector or academia in its cybersecurity work? How effective are these partnerships?
- Does the government provide a platform for information sharing among organizations?
- What guidance on cybersecurity does the government provide to private-sector companies? How clear and coherent is that government advice to multiple stakeholders outside the government?

Are you operationally ready?

Countries vary dramatically in their ability to deal with cyberattacks and how they manage crises. It is often unclear how citizens and businesses should report cyberattacks or seek help. That confusion results in chronic underreporting and makes it hard to know the true scale of the problem and to build understanding to prevent future attacks.

To make matters worse, few countries yet have a workforce with sufficient cybersecurity

skills to match demand. A study of the global information security workforce estimates that the world will fall 1.8 million short of the number of cyberskilled individuals needed by 2022.[3] Those who do have the relevant skills command premium salaries. And what cybersecurity skills others have are often concentrated in small pockets, such as in the intelligence agencies, and not available to governments more broadly. Most governments would do well to invest now in recruitment and training and to adopt more flexible approaches to recruitment and retention from outside traditional sources of talent. For the short term, consolidating existing scarce resources into a single place, as the United Kingdom's NCSC has done, can boost the value of available expertise, bringing the most highly skilled cyberexperts together as a single, government resource.

Some governments are taking a proactive stance on cyberdefense. From 2009, for example, the Australian government consolidated the internet gateways of various departments into seven certified "lead-agency gateways." These provide an initial foundation for consistent cybersecurity and a reduced attack surface.[4] The UK government launched a suite of initiatives in 2017 known as Active Cyber Defence, designed to "protect the majority of people in the UK from the majority of the harm caused by the majority of attacks, the majority of the time." As a result, UK-hosted phishing attacks fell by about 20 percent in the 18 months prior to February 2018, even as global volume itself rose by nearly 50 percent.[5]

Law-enforcement capabilities are often the least effective part of a government's response. Law-enforcement agencies spend up to 95 percent[6] of their budgets on staff, allowing only limited investment in technology. Staffing models are often highly traditional, making it more difficult to bring new technical skills into the organization at the scale and pace needed to address the volume of business that is cybercrime. Criminal-investigation techniques, such as seizure of company servers in evidence, can hinder recovery from attack.

Questions governments can ask include the following:

- What are the emergency-response arrangements for a major cyberattack?
- Is there a national emergency-response team? Are there emergency-response teams for key sectors?
- What arrangements are there for the sharing of information to prevent and respond to a cyberattack? Are there clear reporting mechanisms for alerting the authorities to a cyberattack? What happens when a report is received?
- How often are response arrangements tested and exercised?
- How will the government ensure rapid recovery from a cyberattack?
- Which agency or agencies have responsibility for investigation of cyberattacks and online crime? What capabilities and capacity do those agencies have?
- What capabilities and capacity does the government have to gather intelligence on cyberthreats, assess them, and disseminate the analyses in a way that shapes action?

Where is multinational cooperation possible?

The transnational nature of cyberattacks means that even effective state or national coordination might not be sufficient. Mutual legal-assistance treaties were constructed for the predigital age, and mechanisms are too slow to keep pace with investigation of online crime. In 2013, a UN report on cybercrime estimated that mutual legal assistance took 150 days on average.[7]

Differences in political and ideological positions might make further progress on establishing international norms for the internet impossible. Instead, norms agreed by coalitions—such as the Tallinn Manual, sponsored initially by NATO—might emerge to shape responses to state-based attacks. Bilateral partnerships between other states, such as the one between the Czech Republic and Israel that focuses on the protection of critical assets and encourages private-sector innovation, are also developing. And a proposal before the European Parliament would strengthen its Agency for Network and Information Security in leading the union's cybersecurity efforts, including by having the agency act as a coordination hub for crises.

Questions governments can ask include the following:

- In which international forums on cybersecurity does the government participate?
- What arrangements with other nations does the government have to share information, best practices, or alerts?
- Does the government collaborate with other governments to prevent or investigate cybercrime? How effectively does it use mutual-legal-assistance mechanisms for cybercrime?

How have you defined critical national infrastructure?

If governments address no other aspect of cybersecurity, they must protect critical infrastructure. Many, such as the United States, have started to address cybersecurity from this perspective.[8]

What exactly constitutes critical infrastructure and the proper role of government in protecting it is not universally agreed upon. Some countries, such as France and Israel, have a centralized, regulatory approach toward companies perceived as critical. Both have legislation defining what is critical and related obligations. France formally designates both public and private companies as critical operators, which must then meet a range of specified security requirements—and it defines the category broadly to include more than 250 public and private operating companies across 12 sectors.[9] Others, such as Switzerland, are more decentralized. In the United States, the Department of Homeland Security coordinates a national infrastructure-protection plan and requires sector-specific agencies to develop sector-specific plans. The Office of Infrastructure Protection offers tools and training for companies that are considered critical infrastructure. In the Czech Republic, the implementation of a cybersecurity legal framework has facilitated a more directive approach.

The digital world extends the definition of critical national infrastructure, lengthening the list of sectors and activities that are essential to the smooth functioning of the economy. Companies within those sectors might also have critical dependencies on other organizations, themselves outside the definition of critical national infrastructure. Yet few countries have domestic hardware and software

industries of any scale, leaving them potentially vulnerable to cyberattack through foreign-owned infrastructure. Government decisions about inward investment might increasingly have to balance economic advantage with cybersecurity considerations.

Questions governments can ask include the following:

- Is there an agreed-upon definition of the critical national infrastructure?
- By what means does the government ensure the cybersecurity of critical infrastructure?
- How does the government support the companies and organizations it defines as critical?
- How does the government ensure compliance with security standards? How is that compliance measured?
- Is there a mechanism to ensure that cybersecurity is taken into account when considering major foreign-investment propositions?

Government's role in cybersecurity will only grow as the global demand and dependency on the internet and internet-connected devices continue to increase. With increasing threats and fewer opportunities to fail, governments must rise to the challenge to protect both national security and economic prosperity. ■

[1] *Real lives, real crimes: A study of digital crime and policing*, Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, December 2015, justiceinspectorates.gov.uk.

[2] "Notifiable data breaches scheme," Office of the Australian Information Commissioner, oaic.gov.au.

[3] *2017 Global Information Security Workforce Study*, Center for Cyber Safety and Education, iamcybersafe.org.

[4] "ASD certified gateways," Australian Signals Directorate, February 2017, acsc.gov.au.

[5] Ian Levy, "Active Cyber Defence – one year on," UK National Cyber Security Center, February 5, 2018, ncsc.gov.uk.

[6] Review of published police-department budgets.

[7] "The mutual legal assistance problem explained," blog entry by Gail Kent, February 23, 2015, cyberlaw.stanford.edu.

[8] Interview with Daniel Prieto, former director of cybersecurity and technology, US National Security Council.

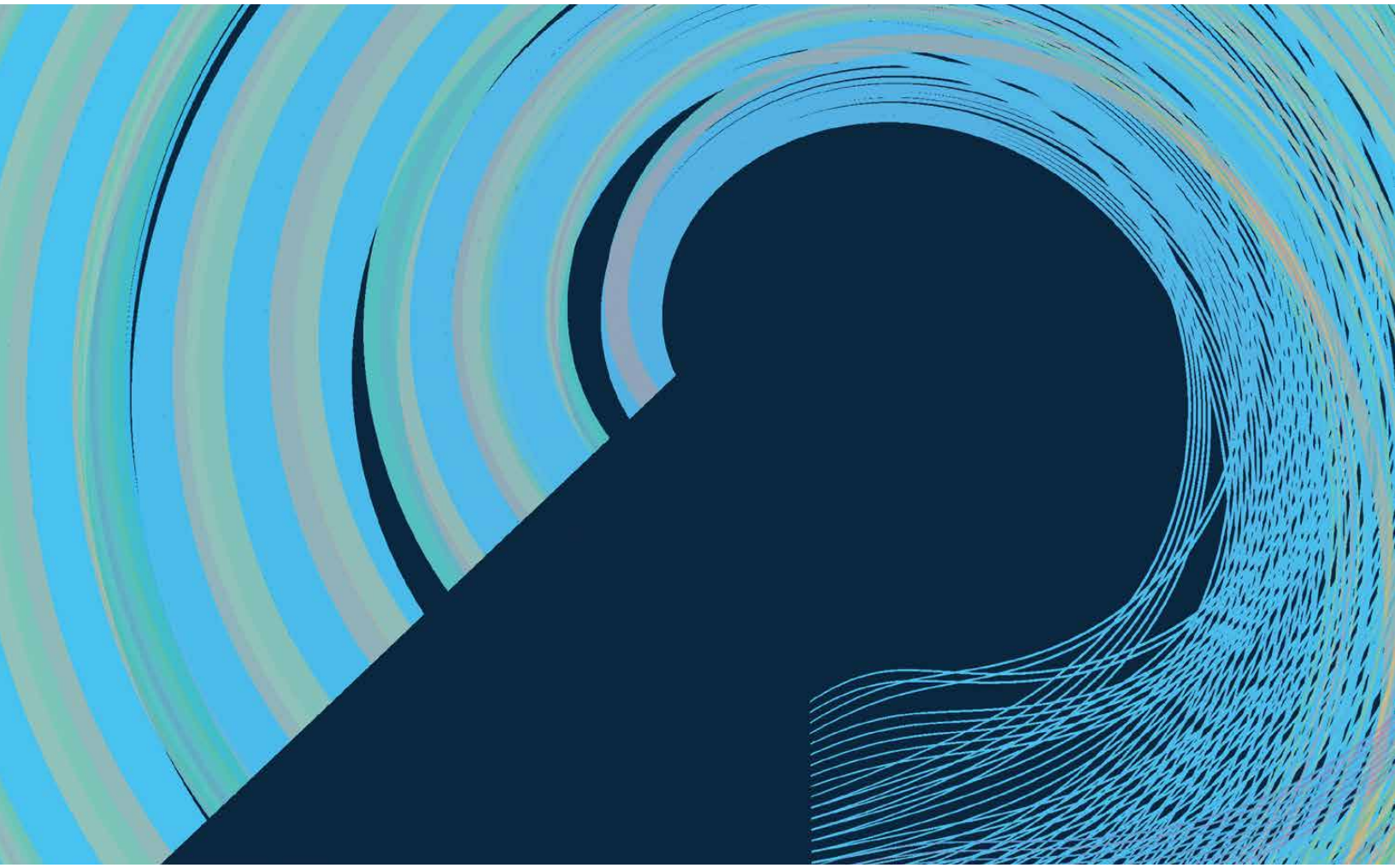
[9] *The critical infrastructure protection in France*, Secrétariat Général de la Défense et de la Sécurité Nationale, January 2017, sgdsn.gouv.fr.

Mary Calam is a senior expert in McKinsey's London office, where **David Chinn** is a senior partner and **John Noble** is an external adviser, and **Jonathan Fantini Porter** is a specialist in the Washington, DC, office.

Value and resilience through better risk management

In a risk environment that is growing more perilous and costly, boards need to help steer their companies toward resilience and value by embedding strategic risk capabilities throughout the organization.

Daniela Gius, Jean-Christophe Mieszala, Ernestos Panayiotou, and Thomas Poppensieker



Today's corporate leaders navigate a complex environment that is changing at an ever-accelerating pace. Digital technology underlies much of the change. Business models are being transformed by new waves of automation, based on robotics and artificial intelligence. Producers and consumers are making faster decisions, with preferences shifting under the influence of social media and trending news. New types of digital companies are exploiting the changes, disrupting traditional market leaders and business models. And as companies digitize more parts of their organization, the danger of cyberattacks and breaches of all kinds grows.

Beyond cyberspace, the risk environment is equally challenging. Regulation enjoys broad popular support in many sectors and regions; where it is tightening, it is putting stresses on profitability. Climate change is affecting operations and consumers and regulators are also making demands for better business conduct in relation to the natural environment. Geopolitical uncertainties alter business conditions and challenge the footprints of multinationals. Corporate reputations are vulnerable to single events, as risks once thought to have a limited probability of occurrence are actually materializing.

The role of the board and senior executives

Risk management at nonfinancial companies has not kept pace with this evolution. For many nonfinancial corporates, risk management remains an underdeveloped and siloed capability in the organization, receiving limited attention from the most senior leaders. From more than 1,100 respondents to McKinsey's Global Board Survey for 2017, we discovered that risk management remains a relatively low-priority topic at board meetings (exhibit).

Boards spend only 9 percent of their time on risk—slightly less than they did in 2015. Other questions in the survey revealed that only 6 percent of respondents believe that they are effective in managing risk (again, less than in 2015). Some individual risk areas are relatively neglected, and even cybersecurity, a core risk area with increasing importance, is addressed by only 36 percent of

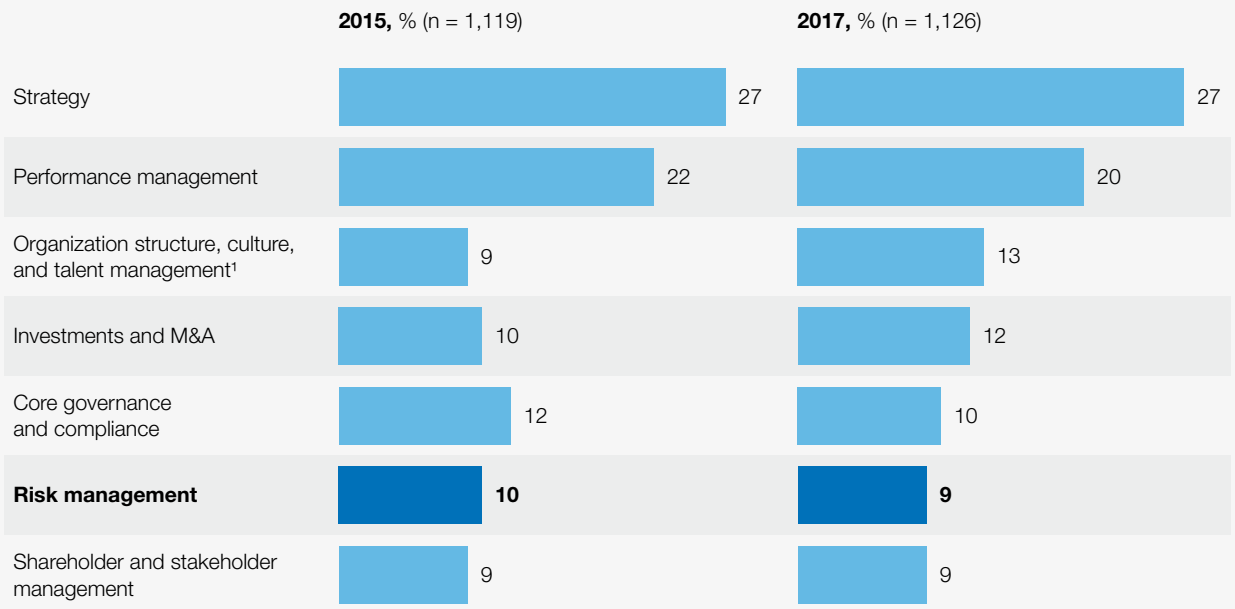
A long way to go

In 2016, McKinsey interviewed a sample of large listed companies in the United Kingdom that had included viability statements in their annual reports. The viability statement—a reporting requirement for London listed companies introduced in 2014—is designed to provide investors with an assessment of the long-term viability of the company. Responses revealed that many non–financial services corporates had never before modeled the impact of an adverse scenario on their financials prior to the new reporting requirement.

Some of the companies that undertook analytical exercises on the impact of macroeconomic variables as part of their analysis for the statement had not also modeled for individual crises, such as a cybersecurity attack. Furthermore, most of the non–financial services companies that we interviewed had not yet used the lessons and insights from analytical exercises to inform their strategic decision making.

Exhibit **McKinsey surveys of more than 1,100 leading global companies reveal that boards devote a relatively small share of time to risk management.**

"Please indicate the % of time your board spends on the following topics during its meetings"



Note: Figures may not sum to 100%, because of rounding

[1] In the past, this category was called "organizational health and talent management."

Source: McKinsey Global Board Survey, April 2015 and 2017

boards. While many senior executives stay focused on strategy and performance management, they often fail to challenge capabilities or strategic decisions from a risk perspective (see sidebar "A long way to go"). A reactive approach to risks remains too common, with action taken only after things go wrong. The result is that boards and senior executives needlessly put their companies at risk, while personally taking on higher legal and reputational liabilities.

Boards have a critical role to play in developing risk-management capabilities at the companies they oversee. First, boards need to ensure that a robust risk-management operating model is in place. Such a model allows companies to understand and prioritize risks, set their risk appetite, and measure their performance against these risks. The model should enable the board and senior executives to work with businesses to eliminate exposures outside the company's appetite statement, reducing the risk profile where warranted through such means as quality controls and other operational processes. On strategic opportunities and risk trade-offs, boards should foster explicit discussions and decision making among top management and the businesses. This will enable the efficient deployment of scarce risk resources and the active, coordinated

management of risks across the organization. Companies will then be prepared to address and manage emerging crises when risks do materialize.

A sectoral view of risks

Most companies operate in a complex, industry-specific risk environment. They must navigate macroeconomic and geopolitical uncertainties and face risks arising in the areas of strategy, finance, products, operations, and compliance and conduct. In some sectors, companies have developed advanced approaches to managing risks that are specific to their business models. These approaches can sustain significant value. At the same time companies are challenged by emerging types of risks for which they need to develop effective mitigation plans; in their absence, the losses from serious risk events can be crippling.

- *Automotive companies* are controlling supply-chain risks with sophisticated monitoring models that allow OEMs to identify potential risks upfront across the supply chain. At the same time, auto companies must address the strategic challenge of shifting toward electric-powered and autonomous vehicles.
- *Pharma companies* seek to manage the downside risk of large investments in their product portfolio and pipeline, while addressing product quality and patient safety to comply with relevant regulatory requirements.
- *Oil and gas, steel, and energy companies* apply advanced approaches to manage the negative effects of financial markets and commodity-price volatility. As social and political demands for cleaner energy are increasing, these companies are actively pursuing growth opportunities to shift their portfolios in anticipation of an energy transition and a low-carbon future.
- *Consumer-goods companies* protect their reputation and brand value through sound practices to manage both product quality and labor conditions in their production facilities. Yet they are constantly challenged to meet consumers' ever-changing tastes and needs, as well as consumer-protection regulations.

Toward proactive risk management

An approach based on adherence to minimum regulatory standards and avoidance of financial loss creates risk in itself. In a passive stance, companies cannot shape an optimal risk profile according to their business models nor adequately manage a fast-moving crisis. Eschewing a risk approach comprised of short-term performance initiatives focused on revenue and costs, top performers deem risk management as a strategic asset, which can sustain significant value over the long term. Inherent in the proactive approach are several essential components.

Strategic decision making

More rigorous, debiased strategic decision making can enhance the longer-term resilience of a company's business model, particularly in volatile markets or externally challenged industries. Research shows that the active, regular reevaluation of resource allocation, based on sound assessments of risk and return trade-offs (such as entering markets where the business model is superior to the competition), creates more value and better shareholder returns.[1] Flexibility is empowering in a dynamic marketplace. Many companies use hedging strategies to insure against

market uncertainties. Airlines, for example, have been known to hedge future exposures to fuel-price fluctuations, a move that can help maintain profitability when prices climb. Likewise, strategic investing, based on a longer-term perspective and a deep understanding of a company's core proposition, generates more value than opportunistic moves aiming at a short-term bump in the share price.

Debiasing and stress-testing

Approaches that include debiasing and stress-testing help senior executives consider previously overlooked sources of uncertainty to judge whether the company's risk-bearing capacity can absorb their potential impact. A utility in Germany, for example, improved decision making by taking action to mitigate behavioral biases. As a result, it separated its renewables business from its conventional power-generation operations. In the aftermath of the Fukushima disaster, which sharply raised interest in environmentally friendly power generation, the utility's move led to a significant positive effect on its share price (15 percent above the industry index).

Higher-quality products and safety standards

Investments in product quality and safety standards can bring significant returns. One form this takes in the energy sector is reduced damage and maintenance costs. At one international energy company, improved safety standards led to a 30 percent reduction in the frequency of hazardous incidents. Auto companies with reputations built on safety can command higher prices for their vehicles, while the better reputation created by higher quality standards in pharma creates obvious advantages. As well as the boost in demand that comes from a reputation for quality, companies can significantly reduce their remediation costs—McKinsey research suggests that pharma companies suffering from quality issues lose annual revenue equal to 4 to 5 percent of cost of goods sold.

Comprehensive operative controls

These can lead to more efficient and effective processes that are less prone to disruption when risks materialize. In the auto sector, companies can ensure stable production and sales by mitigating the risk of supply-chain disruption. Following the 2011 earthquake and tsunami, a leading automaker probed potential supply bottlenecks and took appropriate action. After an earthquake in 2016, the company quickly redirected production of affected parts to other locations, avoiding costly disruptions. In high-tech, companies applying superior supply-chain risk management can achieve lasting cost savings and higher margins. One global computer company addressed these risks with a dedicated program that saved $500 million during its first six years. The program used risk-informed contracts, enabling suppliers to lower the costs and risks of doing business with the company. The measures achieved supply assurance for key components, particularly during market shortages, improved cost predictability for components that have volatile costs, and optimized inventory levels internally and at suppliers.

Stronger ethical and societal standards

To achieve standing among customers, employees, business partners, and the public, companies can apply ethical controls on corporate practices end to end. If appropriately publicized and linked to corporate social responsibility, a program of better ethical standards can achieve significant returns in the form of heightened reputation and brand recognition. Customers, for example, are increasingly willing to pay a premium for products

of companies that adhere to tighter standards. Employees too appreciate being associated with more ethical companies, offering a better working environment and contributing to society.

The three dimensions of effective risk management

Ideally, risk management and compliance are addressed as strategic priorities by corporate leadership and day-to-day management. More often the reality is that these areas are delegated to a few people at the corporate center working in isolation from the rest of the business. By contrast, revenue growth or cost savings are deeply embedded in corporate culture, linked explicitly to profit-and-loss (P&L) performance at the company level. Somewhere in the middle are specific control capabilities regarding, for example, product safety, secure IT development and deployment, or financial auditing.

To change this picture, leadership must commit to building robust, effective risk management. The project is three-dimensional: 1) the risk operating model, consisting of the main risk-management processes; 2) a governance and accountability structure around these processes, leading from the business up to the board level; and 3) best-practice crisis preparedness, including a well-articulated response playbook if the worst case materializes.

1. Developing an effective risk operating model

The operating model consists of two layers: an enterprise-risk-management (ERM) framework and individual frameworks for each type of risk. The ERM framework is used to identify risks across the organization, define the overall risk appetite, and implement the appropriate controls to ensure that the risk appetite is respected. Finally, the overarching framework puts in place a system of timely reporting and corresponding actions on

Finding the right level of risk appetite

Companies need to find the right level of risk appetite, which helps ensure long-term resilience and performance. Risk appetite that is too relaxed or too restrictive can have severe consequences on company financials, as the following two examples indicate:

Too relaxed. One nuclear-energy company set its standards for steel equipment in the 1980s and did not review them even when the regulations changed. When the new higher standards were applied to the manufacture of equipment for nuclear-power plants, the company fell short of compliance. An earlier adaptation of its risk appetite and tolerance levels would have been significantly less costly.

Too restrictive. A pharma company set quality tolerances to produce a drug to a significantly stricter level than what was required by regulation. At the beginning of production, tolerance intervals could be fulfilled, but over time, quality could no longer be assured at the initial level. The company was unable to lower standards, as these had been communicated to the regulators. Ultimately, production processes had to be upgraded at a significant cost to maintain the original tolerances.

risk to the board and senior management. The risk-specific frameworks address all risks that are being managed. These can be grouped in categories, such as financial, nonfinancial, and strategic. Financial risks, such as liquidity, market, and credit risks, are managed by adhering to appropriate limit structures; nonfinancial risks, by implementing adequate process controls; strategic risks, by challenging key decisions with formalized approaches such as debiasing, scenario analyses, and stress testing. While financial and strategic risks are typically managed according to the risk-return trade-off, for nonfinancial risks, the potential downside is often the key consideration.

As well as assessing risk based on likelihood and impact, companies must also assess their ability to respond to emerging risks. Capabilities and capacities needed to manage these risks should be evaluated and gaps filled accordingly. Of particular importance in crisis management is the timeliness of an effective response when things go awry. The highly likely, high-impact risk events on which risk management focuses most of its attention often emerge with disarming velocity, catching many companies unawares.

To be effective, the enterprise risk management framework must ensure that the two layers are seamlessly integrated. It does this by providing clarity on risk definitions and appetite as well as controls and reporting.

- *Taxonomy.* A company-wide risk taxonomy should clearly and comprehensively define risks; the taxonomy should be strictly respected in the definition of risk appetite, in the development of risk policy and strategy, and in risk reporting. Taxonomies are usually industry specific, covering strategic, regulatory, and product risks relevant to the industry. They are also determined by company characteristics, including the business model and geographical footprint (to incorporate specific country and legal risks). Proven risk-assessment tools need to be adopted and enhanced continuously with new techniques, so that newer risks (such as cyber risk) are addressed, as well as more familiar risks.

- *Risk appetite.* A clear definition of risk appetite will translate risk-return trade-offs into explicit thresholds and limits for financial and strategic risks, such as economic capital, cash flow at risk, or stressed metrics. In the case of nonfinancial risks like operational and compliance risk, the risk appetite will be based on overall loss limits, categorized into inherent and residual risks (see sidebar "Finding the right level of risk appetite").

- *Risk-control processes.* Effective risk-control processes ensure that risk thresholds for the specified risk appetite are upheld at all levels of the organization. Leading companies are increasingly building their control processes around big data and advanced analytics. These powerful new capabilities can greatly increase the effectiveness and efficiency of risk-monitoring processes. Machine-learning tools, for example, can be very effective in monitoring fraud and prioritizing investigations; automated natural-language processing within complaints management can be used to monitor conduct risk.

- *Risk reporting.* Decision making should be informed with risk reporting. Companies can regularly provide boards and senior

executives with insights on risk, identifying the most relevant strategic risks. The objective is to ensure that an independent risk view, encompassing all levels of the organization, is embedded into the planning process. In this way, the risk profile can be upheld in the management of business initiatives and decisions affecting the quality of processes and products. Techniques like debiasing and the use of scenarios can help overcome biases toward fulfilment of short-term goals. A North American oil producer developed a strategic hypothesis given uncertainties in global and regional oil markets. The company used risk modeling to test assumptions about cash flow under different scenarios and embedded these analyses into the reports reviewed by senior management and the board. Weak points in the strategy were thereby identified and mitigating actions taken.

2. Toward robust risk governance, organization, and culture

The risk operating model must be managed through an effective governance structure and organization with clear accountabilities. The governance model maintains a risk culture that strongly reinforces better risk and compliance management across the three lines of defense—business and operations, the compliance and risk functions, and audit. The approach recognizes the inherent contradiction in the first line between performance (revenue and costs) and risk (losses). The role of the second line is to review and challenge the first line on the effectiveness of its risk processes and controls, while the third line, audit, ensures that lines one and two are functioning as intended.

- *Three lines of defense.* Effective implementation of the three lines involves the sharp definition of lines one and two at all levels, from the group level through the lines of business, to the regional and legal-entity levels. Accountabilities regarding risk and control management must be clear. Risk governance may differ by risk type: financial risks are usually managed centrally, while operational risks are deeply embedded into company processes. The operational risk of any line of business is managed by the business owning the product-development, production, and sales processes. This usually translates into forms of quality control, but the business must also balance the broader impact of risk and P&L. In the development of new diesel engines, automakers lost sight of the balance between compliance risk and the additional cost to meet emission standards, with disastrous results. Risk or compliance functions can only complement these activities by independently reviewing the adequacy of operational risk management, such as through technical standards and controls.

An enhanced risk culture covers mind-sets and behaviors across the organization. A shared understanding is fostered of key risks and risk management, with leaders acting as role models.

- *Reviewing the risk appetite and risk profile.* Of central importance within the governance structure are the committees that define the risk appetite, including the parameters for doing business. These committees also make specific decisions on top risks and review the control environment for enhancements as the company's risk profile changes. Good governance in this case means that risk decisions are considered within the existing divisional, regional, and senior-management governance structure of a company, supported by risk, compliance, and audit committees.

- *Integrated risk and compliance governance setup.* A robust and adequately staffed risk and compliance organization supports all risk processes. The integrated risk and compliance organization provides for single ownership of the group-wide ERM framework and standards, appropriate clustering of second-line functions, a clear matrix between divisions and control functions, and centralized or local control as needed. A clear trend is observable whereby the ERM layer responsible for group-wide standards, risk processes, and reporting becomes consolidated, whereas the expert teams setting and monitoring specific control standards for the business (including standards for commercial, technical compliance, IT, or cyber risks) become specialized teams covering both regulatory compliance as well as risk aspects.

- *Resources.* Appropriate resources are a critical factor in successful risk governance. The size of the compliance, risk, audit, and legal functions of nonfinancial companies (0.5 for every 100 employees, on average), are usually much smaller than those of banks (6.9 for every 100 employees). The disparity is partly a natural outcome of financial regulation, but some part of it reflects a capability gap in nonfinancial corporates. These companies usually devote most of their risk and control resources in sector-specific areas, such as health and safety for airlines and nuclear power companies or quality assurance for pharmaceutical companies. The same companies can, however, neglect to provide sufficient resources to monitor highly significant risks, such as cyber risk or large investments.

- *Risk culture.* An enhanced risk culture covers mind-sets and behaviors across the organization. A shared understanding is fostered of key risks and risk management, with leaders acting as role models. Especially important are capability-building programs on risk as well as formal mechanisms to assess and reinforce sound risk management practices.

3. Crisis preparedness and response

A high-performing, effective risk operating model and governance structure, with a well-developed risk culture, minimize the probability of corporate crises, without, of course, completely eliminating them. When unexpected crises strike at high velocity, multinational companies can lose billions in value in the first days and soon find themselves struggling to keep their market position. A best-in-class risk-management environment provides the ideal conditions for preparation and response.

- *Ensure board leadership.* The most important action companies can take to prepare for crises is to ensure that the effort is led by the board and senior management. Top leadership must define the main expected threats, the worst-case scenarios, and the actions and communications that will be accordingly rolled out. For each threat, hypothetical scenarios

should be developed for how a crisis will unfold, based on previous crises within and beyond the company's industry and region.

- *Strengthen resilience.* By mapping patterns that arose in previous crises, companies can test their own resilience, challenging key areas across the organization for potential weaknesses. Targeted countermeasures can then be developed in advance to strengthen resilience. This crucial aspect of crisis preparedness can involve reviewing and revising the terms and conditions for key suppliers, shoring up financials to ensure short-term availability of cash, or investing in advanced cybersecurity measures to protect essential data and software in the event of failures and breaches.

- *Develop action plans and communications.* Once these assessments are complete and resilience-building countermeasures are in place, the company can then develop action plans for each threat. The plans must be well articulated, founded on past crises, and address operational and technical planning, financial planning, third-party management, and legal planning. Care should be taken to develop an optimally responsive communications strategy as well. The correct strategy will enable frontline responders to keep pace with or stay ahead of unfolding crises. Communications failures can turn manageable crises into irredeemable catastrophes. Companies need to have appropriate scripts and process logic in place detailing the response to crisis situations, communicated to all levels of the organization and well anchored there. Airlines provide an example of the well-articulated response, in their preparedness for an accident or crash. Not only are detailed scripts in place, but regular simulations are held to train employees at all levels of the company.

- *Train managers at all levels.* The company should train key managers at multiple levels on what to expect and enable them to feel the pressures and emotions in a simulated environment. Doing this repeatedly and in a richer way each time will significantly improve the company's response capabilities in a real crisis situation, even though the crisis may not be precisely the one for which managers have been trained. They will also be valuable learning exercises in their own right.

- *Put in place a detailed crisis-response playbook.* While each crisis can unfold in unique and unpredictable ways, companies can follow a few fundamental principles of crisis response in all situations. First, establish control immediately after the crisis hits, by closely determining the level of exposure to the threat and identifying a crisis-response leader, not necessarily the CEO, who will direct appropriate actions accordingly. Second, involved parties—such as customers, employees, shareholders, suppliers, government agencies, the media, and the wider public—must be effectively engaged with a dynamic communications strategy. Third, an operational and technical "war room" should be set up, to stabilize primary threats and determine which activities to sustain and which

to suspend (identifying and reaching out to critical suppliers). Finally, a deliberate effort must be made to address and neutralize the root cause of the crisis and so bring it to an end as soon as possible.

In a digitized, networked world, with globalized supply chains and complex financial interdependencies, the risk environment has grown more perilous and costly. A holistic approach to risk management, based on the lessons, good and bad, of leading companies and financial institutions, can derive value from that environment. The path to risk resilience that is emerging is an effort, led by the board and senior management, to establish the right risk profile and appetite. Success depends on the support of a thriving risk culture and state-of-the-art crisis preparedness and response. Far from minimal regulatory adherence and loss avoidance, the optimal approach to risk management consists of fundamentally strategic capabilities, deeply embedded across the organization.

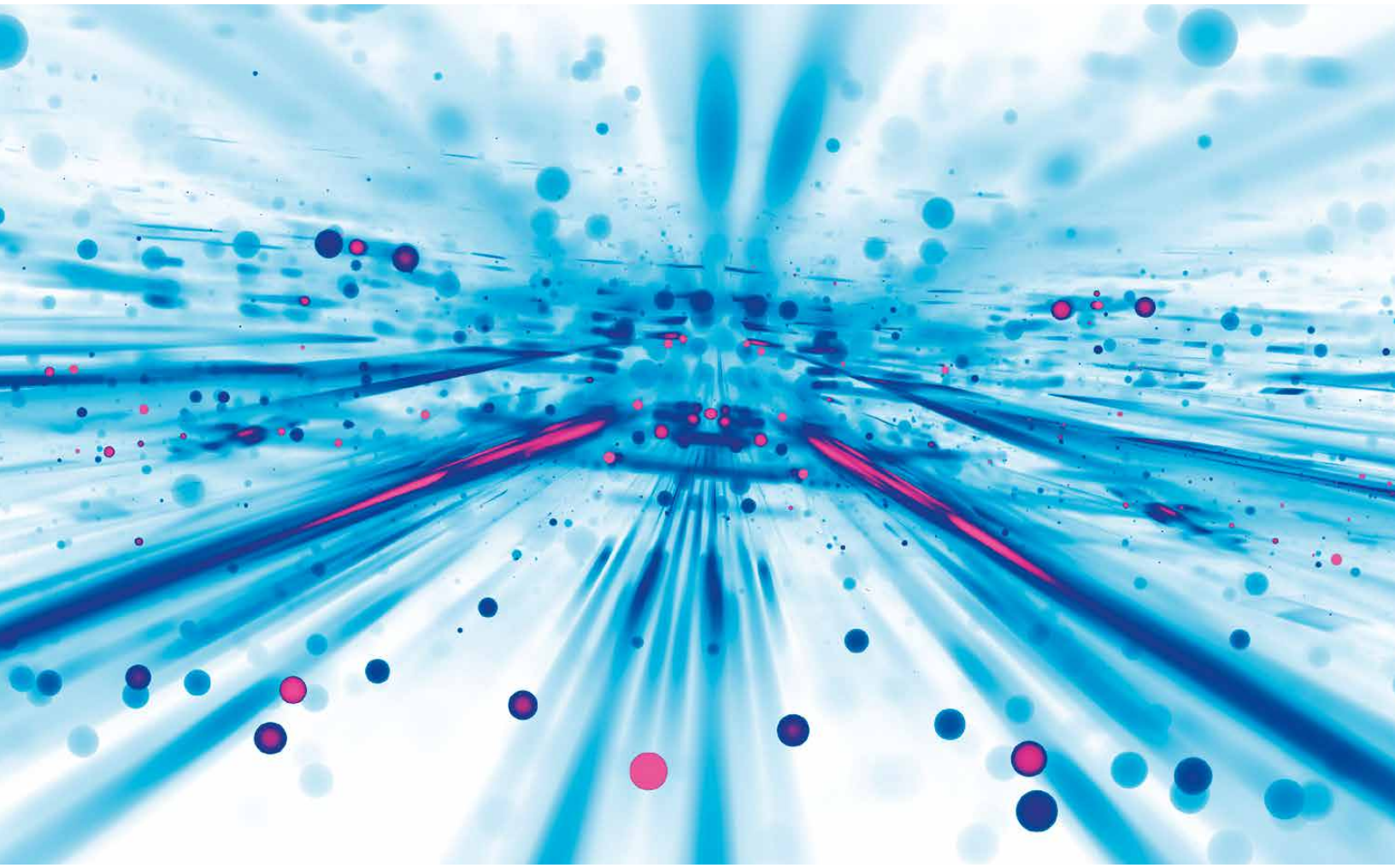
[1] See, for example, Yuval Atsmon, "How nimble resource allocation can double your company's value," August 2016, McKinsey.com; William N. Thorndike, Jr., *The Outsiders: Eight Unconventional CEOs and Their Radically Rational Blueprint for Success,* Boston, MA: Harvard Business Review Press, 2012; Rebecca Darr and Tim Koller, "How to build an alliance against corporate short-termism," January 2017, McKinsey.com.

Daniela Gius is a senior expert in McKinsey's Hamburg office, **Jean-Christophe Mieszala** is a senior partner in the Paris office, **Ernestos Panayiotou** is a partner in the Athens office, and **Thomas Poppensieker** is a senior partner in the Munich office.

The advanced-analytics solution for monitoring conduct risk

Advanced analytics and machine learning can help institutions “connect the dots” across customer and other data to detect conduct risk comprehensively and cost-effectively.

Juan Aristi Baquero, Joseba Eceiza, Dmitry Krivin, and Chetan Venkatesh



The fallout from highly visible instances of misconduct—including reputational damage, material losses, and increased regulatory focus—have led financial institutions to treat conduct risk as an important priority. As a risk category, however, conduct has proved difficult to monitor effectively with traditional controls and testing. The varieties of potential misconduct are numerous, and transgressing individuals or whole departments find ever-changing ways to circumvent rules. In addition, sample-based tests such as transactional reviews are not effective in finding isolated instances of misconduct.

Effective misconduct detection requires a new approach, one that can "connect the dots" across individual and team activities. These connections are often hidden in data that derive from multiple sources. They can be revealed by deploying advanced analytics and machine learning to mine the rich data and thereby identify incongruous sales or transaction patterns, misaligned incentives, and inappropriate customer interactions. Frequently underutilized records (such as the transcripts of customer interactions), can be automatically analyzed for potentially inappropriate treatment that customers may have experienced. But advanced-analytics solutions go beyond the detection of past instances of misconduct—by which the damage to an institution, if any, has already been done—to intercept the outlying patterns of activity that could lead to future losses.

What is conduct risk?

The definition of conduct risk varies somewhat by industry and region but can be commonly understood as individual or group actions that could cause unfair outcomes for customers, undermine market integrity, and damage the firm's reputation and competitive position.

Conduct risk has only recently become recognized as a stand-alone risk category, in the aftermath of a number of high-profile incidents of misconduct (and regulatory responses) in retail and commercial banking, capital markets, and wealth management:

- In the United Kingdom, the discovery of a number of episodes of questionable selling practices in retail and small business led the Financial Conduct Authority to publish new regulatory guidance discouraging staff incentives based on sales targets. These changes coincided with a decline of around 40 percent in sales productivity by branch advisers.
- On trading floors, certain individual rogue traders have caused hundreds of millions of dollars in trading losses at several firms around the globe, while others have colluded to undermine market integrity and gain unfair advantages—such as in the London Interbank Offered Rate (LIBOR) fixing case in 2012. The threat of such behavior continues to pose significant reputational and financial risks to major investment banks.
- In the United States, in 2016, the Consumer Financial Protection Bureau and the Office of the Comptroller of the Currency reinforced customer protections against unauthorized account opening or unrequested enrollment in bank services.
- In Canada, several articles were published in national media outlets in March 2017 claiming aggressive sales tactics by the major banks; the allegations led to internal investigations, hearings before the finance committee of the House of Commons, and a review of sales practices by the Financial Consumer Agency of Canada.

- In Australia, the Royal Commission into Misconduct in the Banking Industry was established in 2017 and is scheduled to make its final report in early 2019.

As a result of these incidents and regulatory responses, many banks are reviewing their conduct-risk approaches and some are revising key components, including the definition of conduct risk, risk taxonomy, risk detection and monitoring, policies and procedures, roles and responsibilities, and issue remediation.

Common risk-monitoring approaches are inadequate for conduct risk

Conduct risk is different from most other types of risk because it entails the great variety and complexity of aberrant human (and organizational) behavior. Since its causes are idiosyncratic, it is impossible to capture the essence of conduct risk in a few quantitative measures—such as those employed for other major risk types (whether value at risk for market risk or expected loss for credit risk). Nevertheless, a single instance of misconduct can have severe negative effects on an institution.

Because it is impossible to quantify simply, conduct risk has not been adequately addressed by traditional methods of risk detection. These methods are generally incapable of actively isolating rare instances of misconduct—instances that can nonetheless cause significant harm to financial institutions.

Apart from communications surveillance, an emerging approach primarily used in trading, conduct risk has mainly been monitored with three approaches: monitoring of customer complaints or internal whistle-blower reports; activity testing, such as verification of customer signatures for new-account opening in branches or sample-based call monitoring in contact centers; and rules-based analytics, such as trade alerts used to monitor activities of wealth advisers or trade surveillance in trading.

No matter how institutions apply these three approaches, they find themselves failing to detect conduct-risk issues comprehensively. For instance, while customer complaints and whistle-blower reporting are necessary elements of conduct monitoring, they cannot substitute for a more complete program. They are lagging indicators first of all, providing signals only after damage to an institution has been done. Additionally, a majority of conduct issues, such as inappropriate selling, go unreported by customers, who may not even be aware of the issue. Incidents that are reported are frequently resolved as soon as the customer contacts the institution, without a complaint ever having been filed. Finally, from the slight percentage of incidents for which a complaint is filed, an institution will find it difficult to identify the sources of the majority of incidents. Typically, a small number of employees or departments will have been responsible, but the common approaches won't find them (Exhibit 1).

Similarly, activity-testing controls, such as branch audits or verification of customer consent, have a number of problematic limitations. First, unless conducted on all or nearly all transactions, they will be ineffective in identifying rare instances of sales misconduct. Second, employees are generally aware of controls in place and can avoid them by focusing on untargeted transactional patterns. Finally, controls are usually manual, making coverage of all possible patterns of sales misconduct prohibitively expensive.

Exhibit 1 **Even with several levels of manual checkers and investigators, most methods for monitoring customer complaints fail to identify the few common sources of misconduct.**

The third common approach, rules-based analytics, has also been proven to be an insufficient way to address conduct risk. This approach uses such techniques as trade alerts to monitor wealth-management advisers, or, in retail banking, thresholds to target those originating an excessive number of unfunded accounts. The approach tends to generate a large number of false positive alerts for further—and costly—investigation. It is also easy to dodge, for example, by selling marginally below known thresholds.

These approaches to conduct-risk identification are beset by additional shortcomings. One is that they rely one-sidedly on numerical data. Unstructured data such as customer-call recordings or surveys are rarely used to good effect in the monitoring framework. Another is a tendency to treat individual factors in isolation, without connecting them in sequence. Given the diversity of conduct-risk activities, the most powerful insights lie in the discovery of patterns across multiple sources; for example, employee sales, customer calls, and incentive plans. Together, structured and unstructured sources of data can help institutions address misconduct more accurately, with far fewer false positives.

A better way

To effectively monitor and detect conduct risk, institutions need a new method, one that leverages the power of data from diverse sources, including customer feedback, sales and product data, and performance-management data. An inclusive data model—one that respects all local laws and regulations—will permit institutions to "connect the dots" across the activities of individuals and departments. Machine-learning algorithms can mine a complex data terrain to establish outlying activities and identify potential instances of misconduct. Designated outliers can then be captured automatically from all recorded customer interactions.

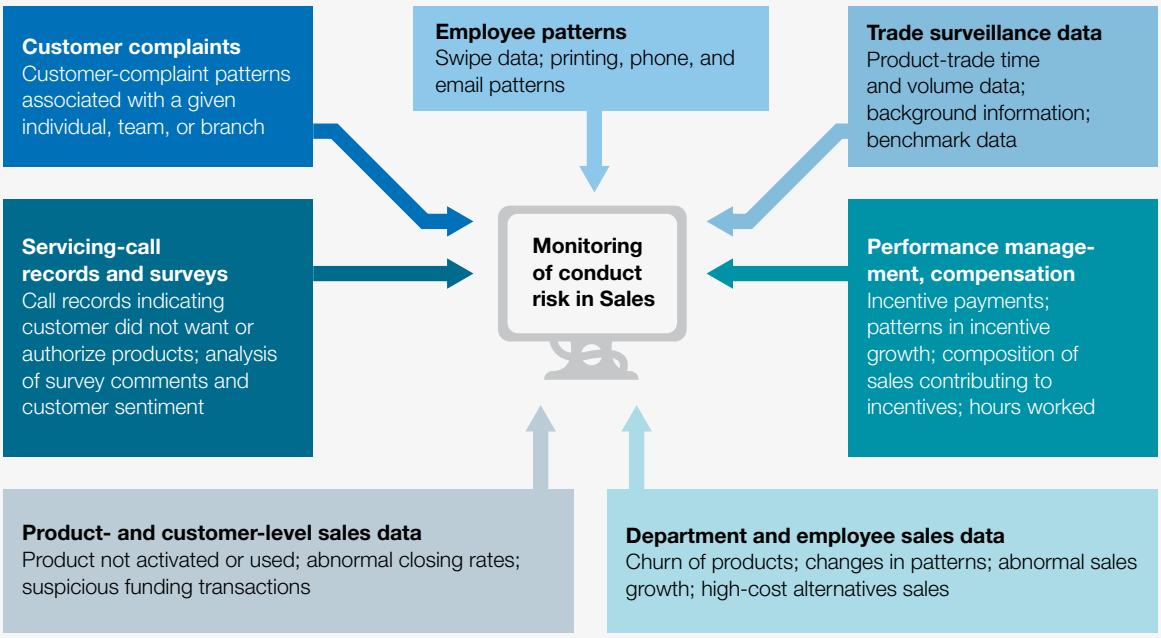
Making use of advances in data and analytics, institutions can transform conduct detection and replace extensive manual controls and verification activities. A number of leading institutions have started on this journey, putting in place monitoring analytics that detect infrequent instances of misconduct, such as inappropriate sales, before significant financial and reputational damage is sustained. An effective conduct-risk analytics monitoring program will be defined by the following capabilities:

1. Connecting the dots across individual activities

A data model can link sales, transaction, and performance data with other sources of insight at the level of individuals and departments (or teams and branches). To build it, organizations need to create data lakes or repositories of structured data (such as sales and account usage) and unstructured data (such as customer-call transcripts, surveys, and complaints). Captured are transactional and sales-performance data, customer patterns (such as portfolio activity for wealth management), and customer intelligence (such as call records to service centers, surveys, complaints). The sources of insight are assembled in granular detail, providing views of the activities of individuals and sales teams or branches. The data are contextualized with additional details, such as management hierarchy and office location. Taken together, the data should fully represent the sales and account activity associated with each individual and can be analyzed systemically to identify suspicious patterns.

Depending on the line of business or type of conduct risk being monitored, other data sources can be included. At the center of the fraud and collusion scandal surrounding the London Interbank Offered Rate in 2012, for example, were traders using chat rooms, instant messaging, and email. Key information from such communications can often be retrieved from corporate-communication platforms and added to the data model. Techniques using advanced analytics can work through this type of data and identify potentially suspicious behavior (Exhibit 2).

Exhibit 2 **The advanced-analytics approach to conduct monitoring 'connects the dots' drawn from many sources of data.**



2. Finding the needle in the haystack

Advanced analytics applied across structured and unstructured data can help classify behavior and detect suspicious or outlying patterns. To develop robust analytics, including machine learning, data scientists work closely with the businesses and control functions to test hypotheses for behaviors defined as indicators for misconduct. This set of analytics will form a control group for identifying outliers. The algorithms are designed to detect these broad patterns, rather than individual instances of misconduct. The approach isolates patterns of activity that the business knows are associated with conduct risk (see sidebar "Mining for patterns associated with conduct risk in wealth management and retail banking").

In addition to mining for known misconduct patterns, machine learning can also be applied to detect previously unknown pattern anomalies. This application, unsupervised learning, is used to mine employee data for new suspicious patterns not identified in the past. For example, a company using unsupervised machine learning identified an employee who was sharing his ID credentials, after the outlier-detection algorithm detected two logins occurring close in time but at locations that were far apart in distance.

Known conduct-risk markers, coupled with unsupervised techniques and additional purely unsupervised techniques for anomaly detection, can be a powerful combination for managing known potential risks and uncovering new and emerging risks. Exhibit 3 illustrates a machine-learning algorithm called the isolation forest, which can identify outlying patterns while distinguishing between positive and negative outliers.

3. Mining customer interactions with natural-language processing

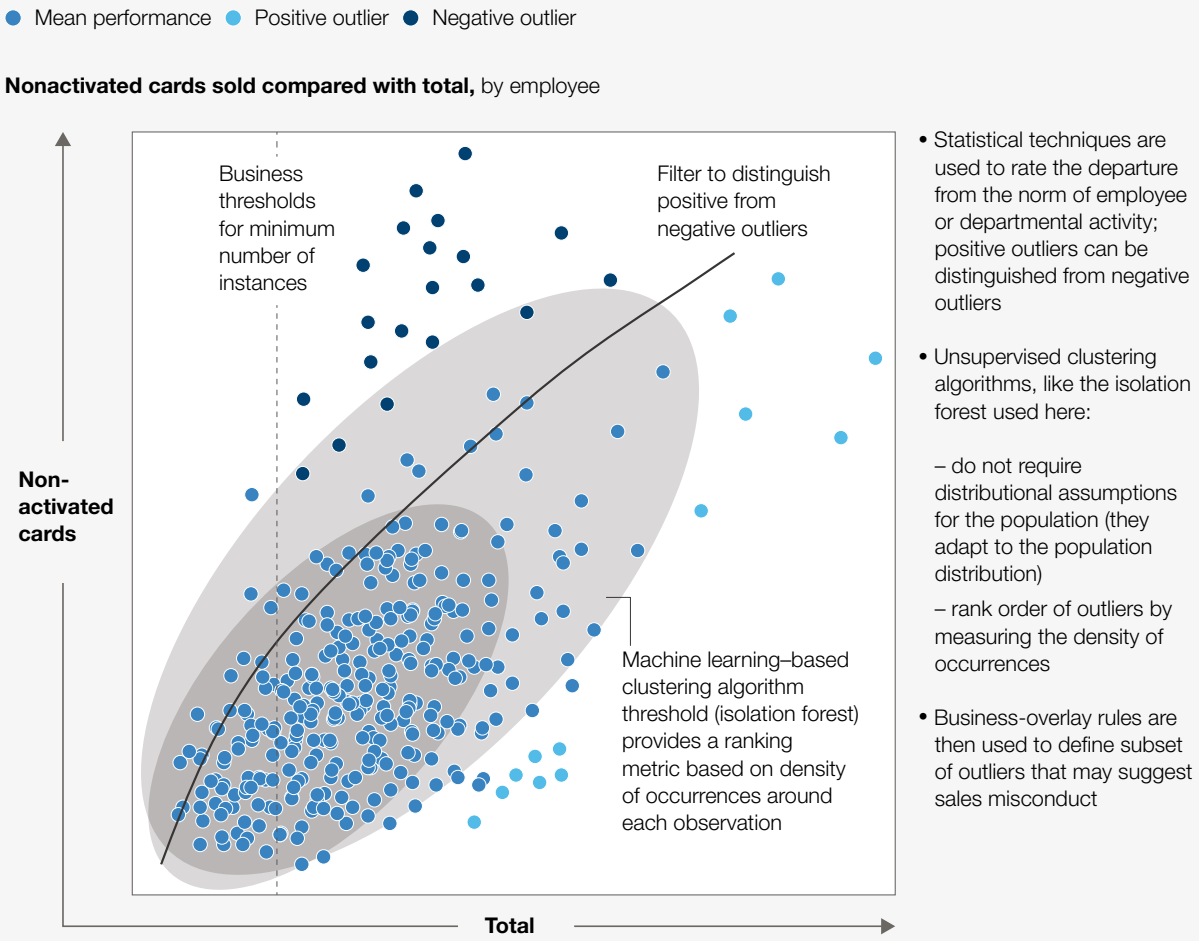
A great amount of data collected from customer interactions with financial institutions is text based, including transcribed phone conversations (see sidebar "Voice-to-text technology"). This kind of data, which is often underutilized, can provide rich insights for conduct-risk detection while also improving the customer experience.

Natural-language processing (NLP) is the branch of artificial intelligence devoted to enabling computers to respond to written or spoken comments and commands given in "natural languages," such as English or Chinese. NLP converts linguistic syntax into computer-readable numeric codes and responds using machine-learning algorithms. Increasingly sophisticated language models have enabled pattern identification within highly specific, tailored contexts. The capabilities of NLP have grown dramatically in the past decade, as has public awareness, with the proliferation of customer-support chatbots and virtual assistants. The application of NLP to text data is a proven approach for analyzing and interpreting customer interactions. The technology can be used to

To develop robust analytics, including machine learning, data scientists work closely with the businesses and control functions to test hypotheses for behaviors defined as indicators for misconduct.

Exhibit 3

Unsupervised machine-learning algorithms such as the isolation forest can detect irregular patterns and filter for potential misconduct.



classify these interactions and identify misconduct, capturing the context of customer dissatisfaction, including its immediate or original source.

In one application, an NLP model worked on a large number of customer surveys (more than 100,000). With and without the use of key words, the model was able to capture instances of potential sales misconduct in customer complaints from several dozen unique surveys. The model highlighted complaints of representatives changing customers' plans without their knowledge, failing sufficiently to explain how products work, and pressuring them to purchase ill-suited products. One complaint specified a hard sell for overdraft protection—including a voluble claim by the teller that it would help the customer's credit rating—despite the customer's insistence that he would

Mining for patterns associated with conduct risk in wealth management and retail banking

Wealth management

Trading and pricing activity

- Excessive churn
- Generation of new sales from rollover products
- Insufficient attention or reverse churn in managed accounts
- Abnormal investment performance compared with clients with similar portfolio composition

Product activation and reversals

- Abnormally high claw-back levels
- Cancellations or reversals of products sold (for example, overdraft, credit protections)
- Excessive sales funded with short-term transfers

Compensation trends

- Abnormal compensation composition or patterns (such as the same or increasing compensation levels with decreasing assets in the portfolio)
- Excess trading near next compensation grid
- Abnormal claw backs due to reversed trades or client gestures

Concentration risk

- Abnormal single-position concentration risk
- Excessive number of unique positions (outside separately managed accounts)
- Suitability: misalignment of portfolio holdings with client risk-appetite statement

Sales-pattern activities

- Outlying growth in sales and incentives, not explained by tenure or hours
- Product and account churn
- Profile of sales skewed toward products with verbal consent

Own account and outside activities

- Excess profitability of own account
- Outside business activities
- Inappropriate investment in private securities

Retail banking

Sales-pattern activities

- Outlying growth in sales or incentives not explained by tenure or hours
- Profile of sales skewed toward products with verbal consent
- Excessive reliance on sales of secondary and tertiary accounts
- Product or service churn on the same account

Product activation and reversals

- Abnormally high claw-back levels
- Downgrades from higher-incentive products
- Cancellations or reversals of products sold (for example, overdraft, credit protection)
- High share of sales of unused products (for example, cards, deposits)

Team-level risk markers

- Team results from operational and compliance reviews
- Team-level complaint trends
- Network shift between branches

Internal risk markers

- Abnormal number of address changes
- High level of products sent to branches at time of sale
- HR referrals related to ethics or sales integrity

Voice-to-text technology

Voice- (or speech-) to-text technology converts audio files of speech to text. The technology has been greatly enhanced recently, through improvements in computing power and the refinement of "deep neural networks." These are sets of algorithms, named after the physiology of thinking, that can cluster and classify large quantities of data in highly sophisticated, customizable ways. The accuracy of transcriptions created using voice-to-text technology has consequently improved dramatically: greater than 90 percent accuracy has been achieved in some test data sets. Better transcriptions of telephone conversations—approaching human accuracy—opens the way to an application of voice-to-text in many use cases, including conduct risk and sales performance.

never use this protection. Another suggested that customers were being signed up for credit insurance without their knowledge. Even taking into account the time needed to develop the model, the automated process saved many hours of human labor in precisely identifying outlying patterns for further investigation.

4. Employee-conduct transparency

By capturing all data on employee conduct and coupling the data with contextual details such as branch, supervisor, and tenure, organizations can build a comprehensive picture of employee performance. As the analyses are targeted at specific behaviors, run on all employees, and normalized through analytic methods, each employee can be compared against the rest of the organization, or a cohort (such as tenure bands). Three useful outcomes can be gleaned from this type of reporting:

- Trends can be identified and specific interventions can be developed before a misconduct case occurs.
- Chronic behavior patterns can be mined and treated with appropriate behavior-improvement training or product controls.
- Systemic and prevalent behaviors can be identified by aggregating the standardized data to supervisor, branch, or district levels.

Overcoming practical challenges

Technological and psychological challenges to developing an analytics-based conduct-risk program may arise. Described here are some common challenges and how they can be resolved.

Insufficient or siloed data. Early in their application of a data strategy, many organizations are unable to monitor employee conduct effectively because they have integrated too little data to build a full picture of employee activity. The initial limitation can be addressed by building out the program gradually, beginning with the most critical data (such as sales and product data, account-activity patterns, and data relating to incentives), and incorporating additional data and analytics over time. Data marts—subject-oriented

databases created for specific purposes—can also be developed, with a view to incorporating them comprehensively or in part, into a data lake over the long term.

Insufficient expertise or resources in data science and advanced analytics. Commonly, banks find that ingoing levels of expertise and resources are insufficient for their analytics ambitions. Overcoming such capability deficits is not difficult, however. Most banks have already created groups of data scientists to develop many forms of machine-learning code, even if they are less familiar with more advanced deep-learning or natural-language-processing algorithms needed for advanced conduct monitoring. These internal resources, complemented with initial external support and/or specific recruiting, can quickly add the required skills as individual use cases are built. Before long, the technical side of conduct-risk monitoring can be managed internally.

Organizational reluctance. Some organizations are reluctant to make a large risk-management investment without evident business benefits. A number of banks have expressed concerns about building conduct-analytics infrastructure for what they see as a purely defensive play, particularly if regulatory examinations did not discover a widespread cause for concern. While the decisions to invest ultimately depend on the risk appetite of each institution, the data and analytics investment described above can generate positive profit-and-loss impact in addition to mitigating risks. First, deploying analytics-based conduct-risk monitoring allows institutions to retire expensive manual controls, testing activities, and investigations of false positives associated with traditional risk-management methods. Second, the same analytics used to mine for conduct risk can also unearth business insights. For instance, the same natural-language-processing engine used to find sales misconduct can also find insights into customer perception of specific products and services. Likewise, data and analytics used to detect suspicious patterns can also identify the sales and behavioral patterns associated with top-performing sales associates. These insights can then be incorporated into training and performance-improvement programs.

■ ■ ■

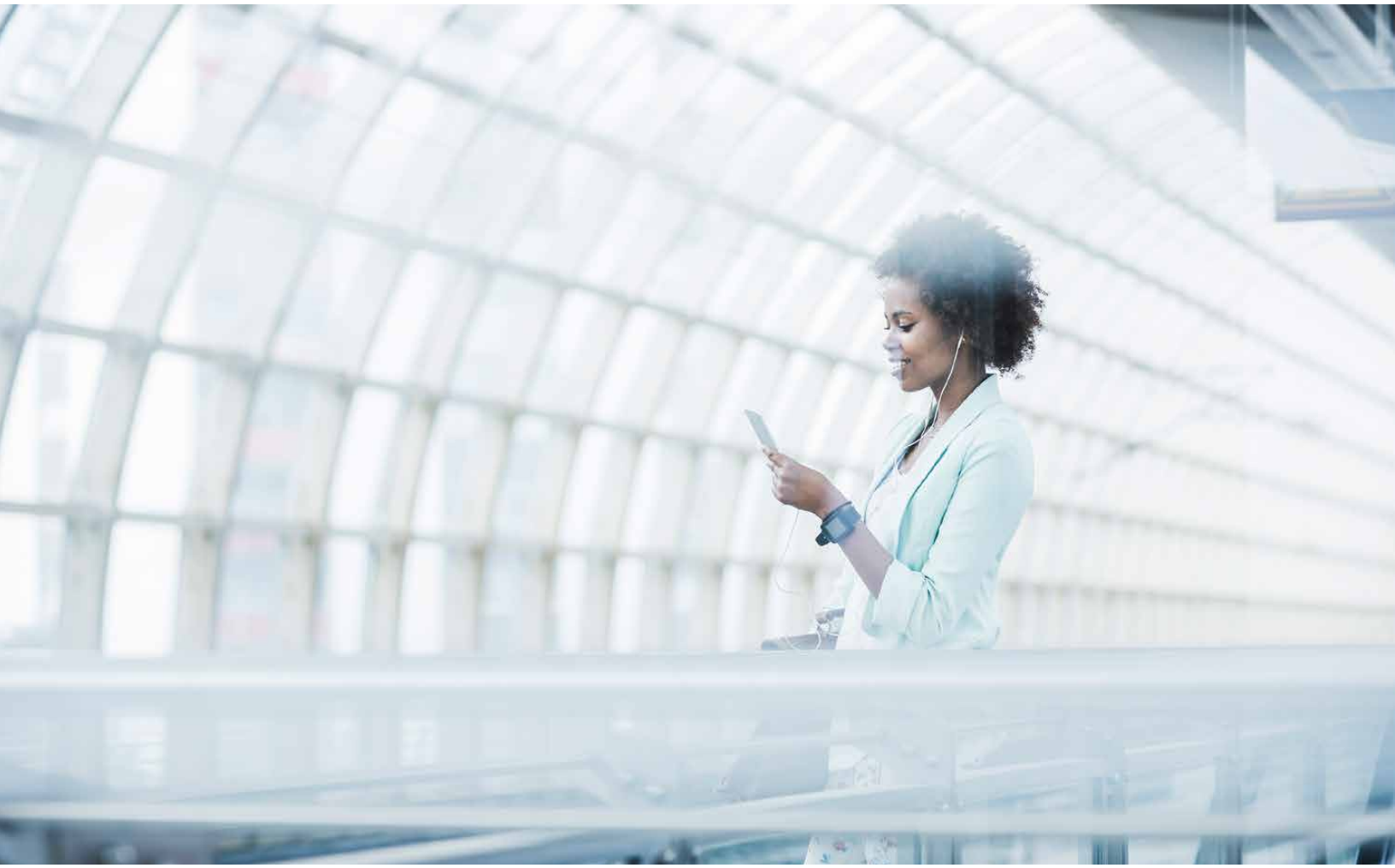
Heightened awareness of business misconduct has affected financial services in challenging ways, exposing even the largest institutions to reputation risk and regulatory scrutiny. Institutions have responded to the challenges, but monitoring the conduct of thousands of employees across many activities, locations, and business units is a complex problem. Fortunately, controls based on advanced analytics and machine learning offer institutions an alternative to a costly infrastructure of manual checkers and investigators. The new approaches enable the effective and efficient monitoring and detection of employee conduct-risk issues before they become serious incidents. A number of advantages accrue to institutions implementing these advanced control programs: they avoid losses of various kinds, they instill confidence in the front line and in regulators by addressing conduct risk in a timely manner, and they create value too, through improved customer relationships. Can you say, "Win-win-win"?■

Juan Aristi Baquero is a partner in McKinsey's New York office, where **Dmitry Krivin** is a partner and **Chetan Venkatesh** is a consultant. **Joseba Eceiza** is a partner in the Madrid office.

The lending revolution: How digital credit is changing banks from the inside

Faster credit decisions, vastly improved customer experience, 40 percent lower costs, and a more secure risk profile. Here's how to get there.

Gerald Chappell, Holger Harreis, Andras Havas, Andrea Nuzzo, Theo Pepanides, and Kayvaun Rowshankish



Today in traditional banks, the average "time to decision" for small business and corporate lending is between three and five weeks.[1] Average "time to cash" is nearly three months. In our view, these times will soon seem as antiquated and unacceptable as the three weeks it once took to cross the Atlantic. Leading banks have embraced the digital-lending revolution, bringing "time to yes" down to five minutes, and time to cash to less than 24 hours.

That's the profound result of a top priority for banks around the world: the digital transformation of end-to-end credit journeys, including the customer experience and supporting credit processes. Credit is at the heart of most customer relationships, and digitizing it offers significant advantages to banks and customers alike. For the bank, successful transformations enhance revenue growth and achieve significant cost savings. One large European bank increased win rates by a third and average margins by more than 50 percent as a result of slashing its time to yes on small- and medium-enterprise (SME) lending from 20 days to less than ten minutes, far outpacing the competition. Our analysis suggests that a bank with a balance sheet of $250 billion could capture as much as $230 million in annual profit,[2] of which just over half derives from cost efficiencies (such as less "touch time" and lower cost of risk), and the remainder comes from revenue gains (increased applications, higher win rates, and better pricing). In this article, we will look at the six design principles that successful banks have used to build digital-lending capabilities and transform their institutions.

The varieties of digital ambition

As digitization proceeds apace, the dimensions of banks' digital ambitions vary among segments and products. Digitization is becoming the norm for retail credit processes. Personal-loan applications can now be submitted with a few swipes on a mobile phone, and time to cash can be as short as a few minutes. Mortgage lending is more complex due to regulatory constraints, yet banks in many developed markets have managed to digitize large parts of the mortgage journey. More than one bank has set an aspiration to automate 95 percent of retail underwriting decisions.

Banks are now treating SME lending as a digital priority. The reasons are clear: costs are high, and the opportunities to improve customer experience are significant. Furthermore, both traditional banks and fintechs already offer compelling digital propositions in SME lending, featuring dramatically shorter approval and disbursement times—a key factor for customers when choosing a lender.

Digital is also advancing in corporate lending, though naturally, corporate banks are moving with greater caution and less urgency (given the relatively lower transaction volumes in this segment). Rather than reworking the entire customer experience, banks are enhancing common processes—for example, digitizing credit-proposal papers and automating annual reviews to improve both time to yes and "quality of yes."

Some banks' digital strategies let corporate-transaction approvers focus their time on those clients and deals that matter the most. Low-risk credit-line renewals, for example, can be automated, while valuable human review time is focused on more complex or riskier deals. And data aggregation can be automated so that relationship managers (RMs) have the most relevant data and risk-monitoring scores at their fingertips—

including financial performance, industry performance, market and sentiment data, and pertinent news and external risk factors.

Avoiding slow starts and piecemeal results

While most banks are digitizing parts of their business and operations, many are dissatisfied with progress, especially in credit. A few familiar frustrations include legacy IT systems; a general lack of trust in automated decision making; insufficient cooperation between businesses and risk, IT, and operations functions; limited data access; and scarce digital talent. Moreover, there is no single "owner" of the credit process with the discretion to drive change at scale. A number of stakeholders need to align and remain constantly aligned over a prolonged period (two to three years in banks that have executed ambitious programs successfully).

These barriers have caused more than one bank to delay or sidetrack digitization efforts. Programs launched with great executive attention and focus lose momentum as the initial excitement of chief risk and lending officers evaporates. Investments needed to sustain programs are partly or wholly withheld. Incremental changes are sometimes substituted for planned end-to-end transformations.

However, numerous banks successfully digitized the credit journey. In the following pages, we offer the practical lessons that have emerged from these experiences, with special emphasis on SME lending, the area that is currently getting the most attention and investment.

Designing a successful digital-lending transformation

Experience has shown that successful transformations rely on some basic principles.

An end-to-end journey but with limited scope

Many banks have found that an end-to-end view of the entire customer journey, including a target state set according to the customer experience, was crucial to success. For example, a Benelux bank redesigned its business-lending process from end to end, allowing it to eliminate numerous handovers. The result was about 30 percent greater efficiency. Without an end-to-end orientation, on the other hand, banks have seen disappointing results. Attempts to improve the credit process piece by piece tend to become incremental, lose customer focus, and miss the big-picture opportunity to deliver a fundamental step change in performance and approach. One Northern European bank found such an opportunity by shifting its focus for SME customers from selling products to fulfilling customer needs. As a result, it radically rationalized its lending-product range down to just three simple products, massively reducing complexity. This would not have happened with a piecemeal approach.

While taking an end-to-end view, however, successful banks have learned that it pays to limit the scope of the first wave of the transformation and focus on a minimum viable product (MVP). The MVP is scoped to be substantial enough to drive real value, momentous enough to create excitement within the organization, and simple enough to be designed and implemented rapidly. Improvements can then be made progressively in waves of rapid subsequent releases.

At one Scandinavian bank, as many as half of all credit decisions concerned SME customers with existing loans seeking additional credit. The bank decided to focus on improving their experience, since the cost to serve them was significant, but the decisions involved were less complex, as most of the necessary data were already available in

the systems. Over an intense 20-week period, the bank designed a new end-to-end digital journey, including an online application process, a framework for making new credit decisions, a revised credit process with automated decision making and fast-track handling for simple cases, as well as radically simplified credit-paper and collateral-review processes. Certain features of the new journey were not included in the MVP but scheduled for later releases. This kind of approach avoids too much early-stage complexity so that a transformative solution can be implemented more quickly, establishing momentum for future change.

Building momentum for full automation

With good reason, risk managers can be wary of a fully automated approval process for business loans. Long-standing policies and decision processes often depend on manual reviews and cross-checks. Years of root-cause analysis of defaults and assessments of soft factors have proved reliable but would be missed in an automated approach.

At one bank in central Europe, the long-standing business-lending process features a decision checklist incorporating thousands of criteria and covenants for contracting and disbursement. While time consuming and costly, the process does achieve the desired risk outcome. In fact, risk functions at many banks successfully use experience-based subjective assessments to achieve low default rates. While the accuracy of data-driven model-based decision making continues to improve, risk managers are correct in taking a cautious approach to automation.

Leading banks express this caution in two ways when introducing automation. First, to establish accuracy, many banks test models on past decisions. A bank in Scandinavia ran its newly developed decision engine on all applications from the past five years. The tests proved that the automated engine based on data-driven assessments and a structured credit "decisioning" framework was better at predicting default risk than the subjective human assessments had been—and far more consistent, which was a key factor in approving the model for use on new cases.

Second, banks start small, at first directing only a few cases to the fully automated straight-through digital process flow (sometimes called the "swim lane"). One Northern European bank recently opened the swim lane for fewer than 15 percent of applications, mainly the less complex cases. As the engine proves itself, the bank will gradually increase the flow.

In the most sophisticated examples, about 70 to 80 percent of SME-lending decisions are fully automated, with the remainder referred for credit review, allowing valuable expert time to be focused on complex or marginal cases.

Embrace relationship managers

RMs play an important role in SME lending. Digitization doesn't replace this. While for some segments it makes sense to steer customers into a mostly self-service approach, successful banks have typically opted for a "multichannel, single application" route for SME lending, where customers can complete digital applications on a shared screen with their RMs. This allows the RM to guide the customer through the process, explain results of automated risk assessments, and quickly ask any follow-up questions required.

A Scandinavian bank went this route, for four reasons:

- In customer testing, it was clear this is what SMEs in the region wanted.
- It allowed the strengthening of RM–customer relationships, and greater cross-selling.
- It allowed the new digital journey to be introduced alongside legacy processes, giving RMs the option of using the old process to give them reassurance (and manage the small number of cases that could not be treated with the new process).
- The digital solution set the right incentives to discourage discounts and lowered the pressure on RMs (by delivering offers in near real time through the digital process, RMs and the bank could gain market share and margin).

Ultimately, RMs were able to provide loan approval in five to ten minutes about three-quarters of the time; more complex cases are decided in an average of 90 minutes (and not more than 24 hours) following a manual review.

Big data—but not too big

To develop models, many banks have expressed interest in using external data (when legally permissible), including novel sources such as social media. While creative use has been made of unusual data sets, it is usually best to begin with readily available data. Transactional data have proved especially powerful. A number of banks and fintechs have developed tools to process transactions from primary operating accounts line by line, classifying them into detailed revenue and expense items. Advanced analytics can use these rich risk data to generate simplified financial statements, affordability ratios, customer- and supplier-concentration analyses, and so on, in real time. These transactional data offer substantially richer and more up-to-date insights about company performance than out-of-date annual accounts. With the second Payment Services Directive (PSD2) and other open-banking initiatives now coming into force, similar analyses can now also be performed on new customers.

Ambitious data-aggregation plans or multiyear data-lake projects are rarely good bases for digital-lending transformations. Such plans are frequently abandoned before completion. Successful transformations generally rely on existing data sources, sometimes using imperfect, robotics-based data integration (such as screen scraping) to get started. Recently, a major bank in Southern Europe successfully completed the early stages of its transformation using readily available demographic and behavioral data. That experience shows how pragmatic data solutions can create real impact quickly, building momentum for subsequent, gradual data-management improvements.

Pragmatic data solutions can create real impact quickly, building momentum for subsequent, gradual data-management improvements.

By incorporating regulatory models in their new credit-decision engines, banks can satisfy regulatory requirements in less time and start reaping the benefits of digitization more quickly. A Northern European bank did just this, after applying the existing internal ratings–based system for business lending and building new automated analyses for affordability and cash flow.

The need for an agile approach

The divergent interests of business and risk management—not to mention operations and IT—will create inherent tensions for banks in redesigning credit processes. One Eastern European bank found that its months-long project to simplify the corporate-lending process had made little headway, ultimately due to legitimate but conflicting internal interests. The project became bogged down with individual silos optimizing for their own interests rather than collaborating on optimizing the customer's experience. It lacked an agile approach.

Agile project delivery is essential for successful credit digitization. The starting point is a set of co-located, cross-functional, full-time, dedicated teams empowered with decision-making authority and tasked to deliver products on deadline in intense bursts of effort called "sprints." However, while most executives are actively talking about agile, not many are actually doing it. Worse, we see many firms adopting "cosmetic agile," where traditional project-management approaches are peppered with agile lingo and walls are filled with Post-it notes referring to agile, but necessary fundamental changes in ways of working are not adopted and organizational commitments are not made.

A common failure is the inability to overcome organizational silos. A cross-functional team with business, risk, IT, and operations is simply essential, for several reasons:

- Collaborating across all functions helps strike the balance of customer-journey and business objectives with robust credit decision making and risk control.
- Bringing critical-path IT-development work into the control of the agile team allows rapid iteration and testing of journeys, data integrations, and results.
- Maintaining agile's customer and "time to market" focus helps quickly assess trade-offs and work-arounds for IT and process bottlenecks as well as design solutions that allow rapid value delivery to customers.

The agile redesign process is sometimes referred to as a "zero-based" approach. Teams begin with a blank sheet rather than thinking about marginal improvements to the existing process and the restrictions of existing policies. They define the essential mission, often working from the customer backward. This mode of operating can initiate deep changes that exceed incremental process adjustments and see beyond the constraints of legacy systems.

A further powerful aspect of agile is the iterative, sprint-based approach to developing solutions. Emerging prototypes are continually tested with RMs and usually clients as well. Teams gather their feedback early on, so that less compelling ideas can be quickly discarded and attention focused on experientially successful ideas—which are also revised as needed. The working relationships fostered in agile teams create enormous engagement among colleagues from all areas of the organization, which ultimately translates into better ideas and faster results.

In a best-practice agile example, a leading European bank built a "digital lab" to enhance its credit processes systematically. Business, IT, and risk came together to align on objectives and incentives, while a dedicated organizational unit (the "digital factory") was empowered to make decisions with quick cross-functional escalation mechanisms. The teams developed a safe IT environment to test changes before reshaping processes on a wider scale.

Consider fintech partnerships

The capability to assess and manage technology partners can be vital to digital-lending transformations. At some banks we have observed that the work-flow engines underlying credit processes cannot be made to support real-time and online lending journeys. In McKinsey's Future of Risk Management Survey,[3] 85 percent of risk managers viewed legacy IT infrastructure as the main challenge in digitization. To address this challenge, many large financial institutions have partnered with fintechs (for example, ING with Kabbage and BBVA Compass Bancshares with OnDeck). The partnerships enable banks to develop new capabilities and present new customer offerings more quickly. Among the assets that fintechs can bring to the partnership are the following:

- full platform capability and data feeds for end-to-end journeys in new markets
- experience in new lending approaches, such as automating SME credit decisions through the use of alternative data sources (such as e-commerce-transaction data from Amazon, PayPal, and eBay; cloud-accounting data from Xero; and banking-transaction data via application programming interfaces from financial-data aggregators such as Yodlee and Finicity)
- individual analytics components, which can be integrated into existing bank processes

The advantages of partnerships have clearly helped one global bank, which developed a digital-lending offering and then worked with an established SME-lending fintech to create the software platform for the customer journey. The software's features include the capability to integrate data from numerous sources and execute automated credit decisioning. While it used the fintech's work-flow engine, the bank retained control over risk appetite by implementing its own decision logic and criteria. The estimate for internal development was a year or more; through the partnership, the project was up and running in four months.

More than 80 percent of top global banks have some form of partnerships with fintechs, of which 16 percent are related to lending. And the success of these partnerships is starting to be recognized. For example, ING and Kabbage partnered in Spain in 2015 to bring platform lending to Europe's small businesses. In 2017, the companies expanded their partnership to France and Italy to support their ability to scale and provide a redefined customer experience.

In pursuing partnerships, banks need to remain clear on partners' primary source of value. If solutions are simply bought off the shelf from vendors, they may lack competitive differentiation and may not fit with an organization's customer profile and business model.

Culture and implementation

The success of a digital-credit transformation rests as much with a managed cultural shift and capable implementation as it does with the design elements we have been discussing.

Managing a cultural shift

Progress in digital-lending transformation occurs when departments and functions with separate priorities are on board. Resistance to change sometimes arises from a general lack of clarity on how digitization will affect the organization and its customers. Senior-management alignment on the goals of the transformation can help counteract emerging cultural issues. A defined end state does more than guide implementation; it can often help overcome opposition to the program. Other elements essential for success include the following:

- *People with the necessary skills,* including data scientists and business "translators," will enable advanced analytics.
- *"Unreasonable" ambitions.* The most successful programs have a "the sky is the limit" culture, refusing to accept any obstacles or restrictions without first challenging them.
- *Visible transformation leaders,* from both business and risk, as well as frontline "champions." Champions are often RMs who are able to convince peers of the benefits of the new digital approach; their feedback on the process will support better solutions.
- *An internal communications strategy* that explains the transformation and the reasons for it will be critical. This can include progress updates communicated electronically as well as organized in-person visits to foster practical cooperation.
- *Pilot testing before enterprise-wide scale-up.* Feedback from the user experience with pilots will provide the basis for refinements and build perception that the solution is a useful new addition to the customer experience.

A practical guide to getting started

Financial institutions that transformed their credit processes took common steps to mobilize their organizations to get there. Here are the distilled elements of successful implementations:

- *Determine the current state.* Measure the lead and approval times in the credit process (touch time, time to cash, and time to yes). Identify potential pain points in major end-to-end credit journeys, such as repeated handoffs, lengthy written reports, reentry of data, process-error rates, and periods of dead time. Know what you're solving for.
- *Determine the right sequence for automation.* The relevant factors for establishing priorities include available material gains ("materiality"), ease of eliminating pain points, and overall complexity in execution. The most common credit journeys selected for automation at the outset of credit transformations are retail mortgages and SME lending (including business banking). The initial focus is usually on existing customers that are refinancing or increasing limits.
- *Learn from leading banks.* Teams can use success stories from leading banks as starting points for proposing innovative ideas and ideal solutions, before working out how these can be made operational. One large Western European banking group gathered its credit experts from various countries to share key elements of its

credit origination and underwriting processes across segments and products. The innovative ideas that participants exchanged became the foundation of a high-level blueprint for the credit journeys of the future.

- *Use the target state to motivate the transformation.* We have emphasized the importance of the destination—the end state of the transformation that has been defined by the business, risk, and operations functions. Supported by compelling value analysis and clear performance targets, this goal can be used to motivate real progress while dispelling potentially crippling misperceptions that digital transformations are not customer focused. A large US bank, for example, set as a goal a two-day limit for coming to conditional decisions on at least 80 percent of all corporate-lending applications.

- *Mobilize the agile team.* The agile team establishes the parameters of the MVP, determines the target IT architecture for the solution, and begins working across functions (business, risk, technology, and operations) on the components of change, following well-defined timetables.

While the challenges in digital-lending transformations are formidable and the path to ultimate success can be bumpy, experience proves that the efforts expended are more than fully repaid in competitiveness and profitability. Success means much faster credit decisions, with customers getting cash up to 80 percent sooner; lower costs, with 30 to 50 percent less time spent on decision making; and better-quality risk decisions, which translate into greater profitability down the road.

[1] Based on data and interviews with approximately 20 financial institutions, mainly in Europe, and some in Asia and North America.

[2] *The future of risk management in the digital era,* a joint report from the Institute of International Finance and McKinsey & Company, December 2017, McKinsey.com.

[3] Ibid.

Gerald Chappell is a partner in McKinsey's London office, **Holger Harreis** is a senior partner in the Düsseldorf office, **Andras Havas** is a partner in the Budapest office, **Andrea Nuzzo** is an associate partner in the Rome office, **Theo Pepanides** is a senior partner in the Athens office, and **Kayvaun Rowshankish** is a partner in the New York office.

Risk Practice leadership

Cindy Levy
Global
Cindy_Levy@McKinsey.com

Hamid Samandari
Americas
Hamid_Samandari@McKinsey.com

Philipp Härle
Western Europe
Philipp_Haerle@McKinsey.com

Gabriel Vigo
Asia
Gabriel_Vigo@McKinsey.com

Gökhan Sari
Eastern Europe, Middle East, North Africa
Gokhan_Sari@McKinsey.com

Kevin Buehler
Risk Advanced Analytics
Kevin_Buehler@McKinsey.com

Marco Piccitto
Risk People
Marco_Piccitto@McKinsey.com

Holger Harreis, Olivia White
Risk Knowledge
Holger_Harreis@McKinsey.com
Olivia_White@McKinsey.com

Thomas Poppensieker
Chair, Global Risk Editorial Board
Thomas_Poppensieker@McKinsey.com

November 2018
Designed by Global Editorial Services

This McKinsey Practice Publication meets the Forest Stewardship Council® (FSC®) chain-of-custody standards. The paper used in this publication is certified as being produced in an environmentally responsible, socially beneficial, and economically viable way.

Printed in the United States of America.