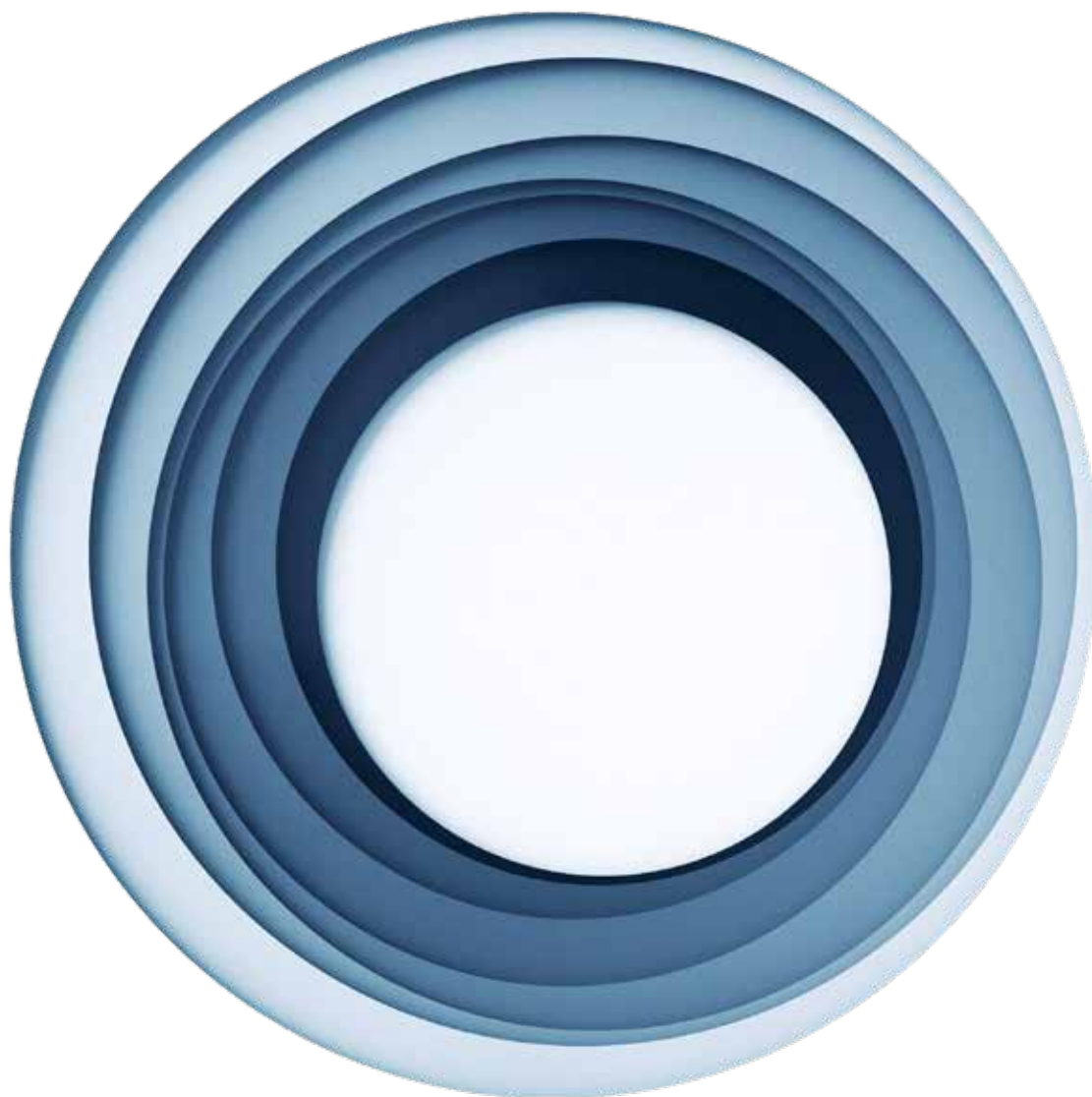


McKinsey  
& Company



# McKinsey on Risk

Financial crime, anti-money  
laundering, and cybersecurity

*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](https://www.mckinsey.com). Comments and requests for copies or for permissions to republish an article can be sent via email to [McKinsey\\_Risk@McKinsey.com](mailto:McKinsey_Risk@McKinsey.com).

Cover image:  
© piranka/Getty Images

**Editorial Board:**

Bob Bartels, Kyra Blessing, Richard Bucci, Philipp Härle, Marie-Paule Laurent, Maria Martinez, Luca Pancaldi, Thomas Poppensieker, Kate Robu, Kayvaun Rowshankish, Roger Rudisuli, Himanshu Singh, Mark Staples, Marco Vettori, Thomas Wallace, John Walsh

**External Relations, Global Risk Practice:** Kyra Blessing

**Editor:** Richard Bucci

**Contributing Editor:**  
Mark Staples

**Art Direction and Design:**  
Leff Communications

**Data Visualization:**  
Richard Johnson,  
Jonathon Rivait

**Managing Editors:**  
Heather Byer,  
Venetia Simcock

**Editorial Production:**  
Elizabeth Brown, Roger Draper,  
Gwyn Herbein, Pamela Norton,  
Katya Petriwsky, Charmaine Rice,  
John C. Sanchez, Dana Sand, Sneha Vats, Pooja Yadav, Belinda Yu

**McKinsey Practice Publications**

**Editor in Chief:**  
Lucia Rahilly

**Executive Editors:**  
Michael T. Borruso,  
Bill Javetski, Mark Staples

Copyright © 2019 McKinsey & Company. All rights reserved.

This publication is not intended to be used as the basis for trading in the shares of any company or for undertaking any other complex or significant financial transaction without consulting appropriate professional advisers.

No part of this publication may be copied or redistributed in any form without the prior written consent of McKinsey & Company.

# Table of contents



## 3 Financial crime and fraud in the age of cybersecurity

As cybersecurity threats compound the risks of financial crime and fraud, institutions are crossing functional boundaries to enable collaborative resistance.

---



## 14 Flushing out the money launderers with better customer risk-rating models

Dramatically improve detection rates by simplifying model architecture, fixing underlying data, and using machine-learning algorithms to identify high-risk behavior.

---



## 21 Scotiabank's chief risk officer on the state of anti-money laundering

Daniel Moore talks about finding bad guys, creating good money, and everything in between.

---



## 27 The risk-based approach to cybersecurity

The most sophisticated institutions are moving from a maturity-based to a risk-based approach for managing cyberrisk. Here is how they are doing it.

---



## 38 Cybersecurity: Linchpin of the digital enterprise

As companies digitize businesses and automate operations, cyberrisks proliferate. Here is how a cybersecurity organization can support a secure digital agenda.

---



## 47 Securing software as a service

Here is how SaaS providers can meet the security needs of their enterprise customers.

---



## 56 The customer mandate to digitize collections strategies

Customers told us that more calling won't improve lenders' contact and recovery rates. Here's what they said does work.

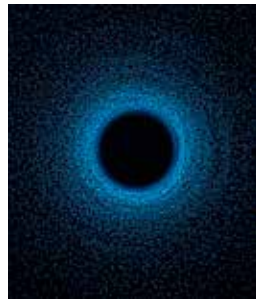
---



## 64 What will Europe's ePrivacy Regulation mean for your business?

The ePrivacy Regulation, an elaboration of the GDPR, has been moving closer to adoption. Beyond preparing for compliance, smart companies can find business advantages.

---



## 69 GDPR compliance since May 2018: A continuing challenge

Companies must automate and streamline, or the challenge of GDPR compliance will overwhelm them.

---

# Introduction

Welcome to the eighth issue of *McKinsey on Risk*, the journal presenting McKinsey's global perspective and strategic thinking on risk. Here you will find articles addressing the principal risk areas affecting the performance of the world's leading companies. Taking a global view across business sectors and functions, our experts offer industry insights and recount hands-on experiences of companies that are transforming risk management and reducing enterprise risk.

This issue puts particular focus on the intersection of cybersecurity and efforts against financial crime, including anti-money laundering programs. The stakes in these areas have never been higher. Hundreds of billions of dollars pass through financial institutions illicitly each year, exploiting automated systems and digitized pathways. Money launderers and defrauders use increasingly sophisticated methods, while the complexity of cybersecurity breaches and attacks has increased, posing a greater threat to institutional integrity. Globally, companies are spending millions of dollars to counter the dangers, while regulatory penalties imposed for perceived laxity have run to tens of billions of dollars.

Our articles discuss the most effective solutions, based on the experiences of the world's leading companies. Going beyond siloed responses, these approaches often involve the risk, compliance, and cybersecurity functions working together with the businesses to improve detection and reduce enterprise risk. Regulators are now supporting innovation, encouraging companies to invest in advanced analytics and artificial intelligence. These powerful tools vastly improve risk effectiveness and efficiency—network analytics, for example, can find the hidden links between entities, illuminating the relationships and interconnected transactions that characterize money-laundering activity.

The overall orientation is entirely consistent with the risk-based approaches that McKinsey has long advocated. Used to their full potential, these approaches create value directly, enhancing business strategies as well as reducing costs. Nowhere is this more apparent than in our risk-based approach to cybersecurity, which enables companies to protect their most valuable assets and conduct operations more safely—and at lower cost—while taking full business advantage of their risk appetite.

We are fully cognizant of the formidable transformation challenges posed by these advanced solutions. Our risk-based approaches thus incorporate the most practical methods for surmounting the challenges and achieving the needed risk transformations. In today's risk environment, we believe that there is no viable alternative.

Let us know what you think at [McKinsey\\_Risk@McKinsey.com](mailto:McKinsey_Risk@McKinsey.com) and on the McKinsey Insights app.

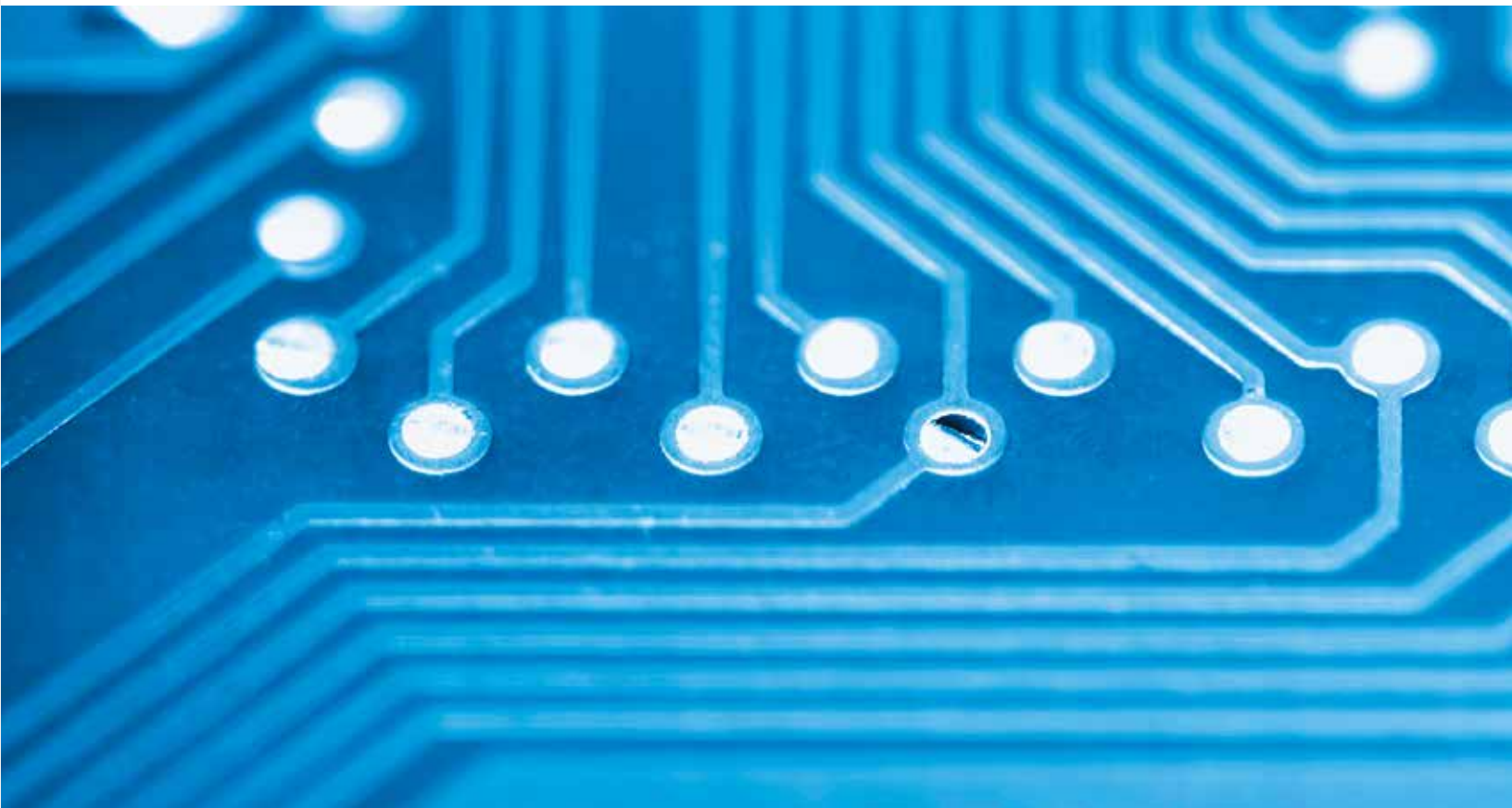


**Thomas Poppensieker**  
*Chair, Global Risk Editorial Board*

# Financial crime and fraud in the age of cybersecurity

As cybersecurity threats compound the risks of financial crime and fraud, institutions are crossing functional boundaries to enable collaborative resistance.

*by Salim Hasham, Shoan Joshi, and Daniel Mikkelsen*



© Cimmerian/Getty Images

In 2018, the World Economic Forum noted that fraud and financial crime was a trillion-dollar industry, reporting that private companies spent approximately \$8.2 billion on anti-money laundering (AML) controls alone in 2017. The crimes themselves, detected and undetected, have become more numerous and costly than ever. Per a widely cited estimate, for every dollar of fraud, institutions lose nearly three dollars, once associated costs are added to the fraud loss itself.<sup>1</sup> Risks for banks arise from diverse factors, including vulnerabilities to fraud and financial crime inherent in automation and digitization, massive growth in transaction volumes, and the greater integration of financial systems within countries and internationally. Cybercrime and malicious hacking have also intensified. In the domain of financial crime, meanwhile, regulators continually revise rules, increasingly to account for illegal trafficking and money laundering, and governments have ratcheted up the use of economic sanctions, targeting countries, public and private entities, and even individuals. Institutions are finding that their existing approaches to fighting

such crimes cannot satisfactorily handle the many threats and burdens. For this reason, leaders are transforming their operating models to obtain a holistic view of the evolving landscape of financial crime. This view becomes the starting point of efficient and effective management of fraud risk.

## The evolution of fraud and financial crime

Fraud and financial crime adapt to developments in the domains they plunder. (Most financial institutions draw a distinction between these two types of crimes; for a view on the distinction, or lack thereof, see sidebar “Financial crime or fraud?”) With the advent of digitization and automation of financial systems, these crimes have become more electronically sophisticated and impersonal.

One series of crimes, the so-called Carbanak attacks beginning in 2013, well illustrates the cyber profile of much of present-day financial crime and fraud. These were malware-based bank thefts

---

<sup>1</sup> World Economic Forum Annual Meeting, Davos-Klosters, Switzerland, January 23–26, 2018; *LexisNexis risk solutions 2018 True Cost of Fraud study for the financial services sector*, LexisNexis, August 2018, risk.lexisnexis.com.

## Financial crime or fraud?

For purposes of detection, interdiction, and prevention, many institutions draw a distinction between fraud and financial crime. Boundaries are blurring, especially since the rise of cyberthreats, which reveal the extent to which criminal activities have become more complex and interrelated. What’s more, the distinction is not based on law, and regulators sometimes view it as the result of organizational silos. Nevertheless, financial crime has generally meant

money laundering and a few other criminal transgressions, including bribery and tax evasion, involving the use of financial services in support of criminal enterprises. It is most often addressed as a compliance issue, as when financial institutions avert fines with anti-money laundering activities. Fraud, on the other hand, generally designates a host of crimes, such as forgery, credit scams, and insider threats, involving deception of financial personnel or services to commit

theft. Financial institutions have generally approached fraud as a loss problem, lately applying advanced analytics for detection and even real-time interdiction. As the distinctions among these three categories of crime have become less relevant, financial institutions need to use many of the same tools to protect assets against all of them.

totaling more than \$1 billion. The attackers, an organized criminal gang, gained access to systems through phishing and then transferred fraudulently inflated balances to their own accounts or programmed ATMs to dispense cash to waiting accomplices (Exhibit 1).

Significantly, this crime was one simultaneous, coordinated attack against many banks. The attackers exhibited a sophisticated knowledge of the cyber environment and likely understood banking processes, controls, and even vulnerabilities arising from siloed organizations and governance. They also made use of several channels, including ATMs, credit and debit cards, and wire transfers. The attacks revealed that meaningful distinctions among cyberattacks, fraud, and financial crime are disappearing. Banks have not yet addressed these new intersections, which transgress the boundary lines most have erected between the types of crimes (Exhibit 2).

A siloed approach to these interconnected risks is becoming increasingly untenable; clearly, the operating model needs to be rethought.

As banks begin to align operations to the shifting profile of financial crime, they confront the deepening connections between cybersecurity breaches and most types of financial crime. The cyber element is not new, exactly. Until recently, for example, most fraud has been transaction based, with criminals exploiting weaknesses in controls. Banks counter such fraud with relatively straightforward, channel-specific, point-based controls. Lately, however, identity-based fraud has become more prevalent, as fraudsters develop applications to exploit natural or synthetic data. Cyber-enabled attacks are becoming more ambitious in scope and omnipresent, eroding the value of personal information and security protections.

Exhibit 1

**The new cyber profile of fraud and financial crime is well illustrated by the Carbanak attacks.**



**1. Spear phishing**  
Employee in targeted organization receives email with the Carbanak backdoor malware as an attachment



**2. Backdoor plan executed; credentials stolen**  
Upon opening attachment, employee activates the Carbanak backdoor malware



**3. Machines infected in search for admin PC**  
Carbanak searches network and finds admin PC; embeds and records



**4. Admin PC identified; clerk screens intercepted**  
Attacker watches admin screen to mimic admin behavior for the bank's cash-transfer systems



**5. Balances inflated; inflated amount transferred**  
Attackers alter balances and pocket extra funds (\$1,000 account enlarged to \$10,000, then \$9,000 transferred)



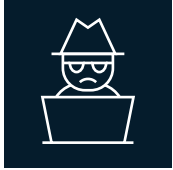
**6. ATM programmed to dispense cash**  
Attackers program ATMs to issue cash to waiting accomplices at specific times



**7. Cash moved through channels by wire transfers and e-payments**  
Attackers use online and electronic payments to receiver banks to transfer extracted funds

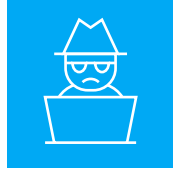
**Crime pathways are converging, blurring traditional distinctions among cybersecurity breaches, fraud, and financial crime.**

**Fraud and insider threats**



- Internal and external threats
- Retail and nonretail threats
- Insider threats
- Market abuse and misbehavior

**Cybersecurity breaches**



- Confidentiality
- Integrity
- Systems availability

**Financial crimes**



- Money laundering
- Bribery and corruption
- Tax evasion and tax fraud

**Example: cyberattack on a central bank**

- Bank employee's SWIFT<sup>1</sup> credentials stolen with the help of insiders
- Malware surreptitiously installed on the bank's computers to prevent discovery of withdrawals
- Funds routed from the bank's account at a branch of another country's central bank to a third bank (on a weekend to ensure staff absence)
- Withdrawals made at the third bank through multiple transactions that were not blocked until too late
- Attacks may have been linked to a known sanctioned entity

<sup>1</sup> Society for Worldwide Interbank Financial Telecommunication.

In a world where customers infrequently contact bank staff but rather interact almost entirely through digital channels, “digital trust” has fast become a significant differentiator of customer experience. Banks that offer a seamless, secure, and speedy digital interface will see a positive impact on revenue, while those that don't will erode value and potentially lose business. Modern banking demands faster risk decisions (such as real-time payments), so banks must strike the right balance between managing fraud and handling authorized transactions instantly.

The growing cost of financial crime and fraud risk has also overshot expectations, pushed upward by several drivers. As banks focus tightly on reducing liabilities and efficiency costs, losses in areas such as customer experience, revenue, reputation, and even regulatory compliance are being missed (Exhibit 3).

**Bringing together financial-crime, fraud, and cybersecurity operations**

At leading institutions, the push is on to bring together efforts on financial crime, fraud, and cybercrime. Both the frontline and back-office

operations are oriented in this direction at many banks. Risk functions and regulators are catching on as well. AML, while now mainly addressed as a regulatory issue, is seen as being on the next horizon for integration. Important initial steps for institutions embarking on an integration effort are to define precisely the nature of all related risk-management activities and to clarify the roles and responsibilities across the lines of defense. These steps will ensure complete, clearly delineated coverage—by the businesses and enterprise functions (first line of defense) and by the risk function, including financial-crime, fraud, and cybersecurity operations (second line)—while eliminating duplication of effort.

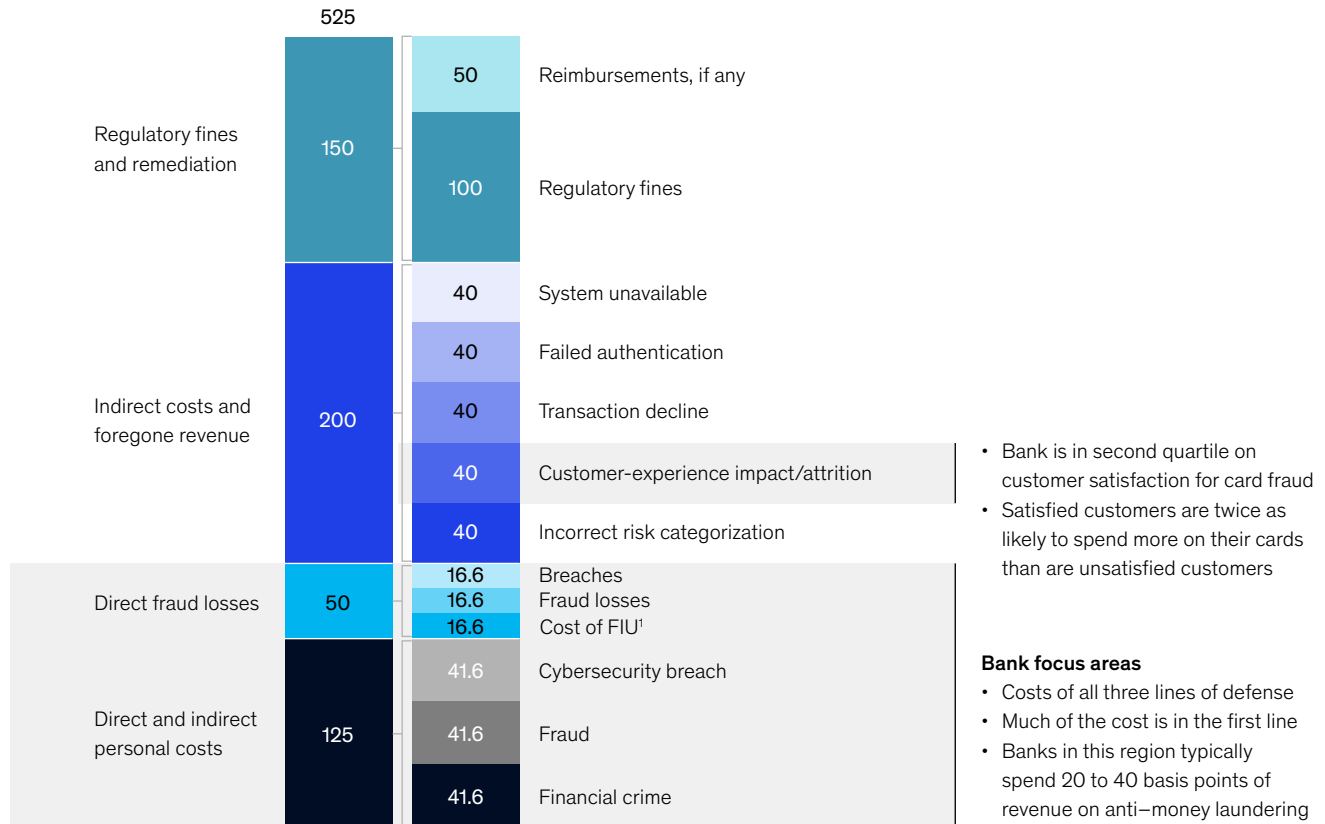
All risks associated with financial crime involve three kinds of countermeasures: identifying and authenticating the customer, monitoring and detecting transaction and behavioral anomalies, and responding to mitigate risks and issues. Each of these activities, whether taken in response to fraud, cybersecurity breaches or attacks, or other financial crimes, are supported by many similar data and processes. Indeed, bringing these data sources together with analytics materially



Exhibit 3

**Banks often focus on only a fraction of total financial-crime, fraud, and cybersecurity costs.**

**Example of financial-crime, fraud, and cybersecurity costs, \$ million**



Note: Figures may not sum to listed totals, because of rounding.

<sup>1</sup> Financial intelligence unit.

improves visibility while providing much deeper insight to improve detection capability. In many instances, it also enables prevention efforts.

In taking a more holistic view of the underlying processes, banks can streamline business and technology architecture to support a better customer experience, improved risk decision making, and greater cost efficiencies. The organizational structure can then be reconfigured as needed (Exhibit 4).

Three models for addressing financial crime are important for our discussion. They are distinguished by the degree of integration they represent among processes and operations for the different types of crime (Exhibit 5).

Generally speaking, experience shows that organizational and governance design are the main considerations for the development of the operating model. Whatever the particular choice, institutions will need to bring together the right people in agile teams, taking a more holistic approach to common processes and technologies and doubling down on analytics—potentially creating “fusion centers,” to develop more sophisticated solutions. It is entirely feasible that an institution will begin with the collaborative model and gradually move toward greater integration, depending on design decisions. We have seen many banks identify partial integration as their target state, with a view that full AML integration is an aspiration.

**At the core, all functions perform the same three roles using similar data and processes.**

	<b>Identification: “Who is my customer?”</b>	<b>Monitoring: “What transactions are legitimate?”</b>	<b>Response: “How do I respond to a threat?”</b>
<b>Financial crime</b>	<ul style="list-style-type: none"> <li>• Client risk rating</li> <li>• Client due diligence; enhanced due diligence</li> </ul>	<ul style="list-style-type: none"> <li>• Transaction monitoring</li> <li>• Name screening</li> <li>• Payments screening</li> </ul>	<ul style="list-style-type: none"> <li>• Suspicious-activity monitoring</li> <li>• Financial intelligence unit</li> <li>• List management</li> <li>• Do not bank</li> </ul>
<b>Fraud</b>	<ul style="list-style-type: none"> <li>• Identity verification, including digital and nondigital presence</li> </ul>	<ul style="list-style-type: none"> <li>• Transaction monitoring and decision making</li> <li>• Device and voice analytics</li> </ul>	<ul style="list-style-type: none"> <li>• Investigations and resolutions teams</li> </ul>
<b>Cybersecurity</b>	<ul style="list-style-type: none"> <li>• Credentials management</li> </ul>	<ul style="list-style-type: none"> <li>• Security-operations center (SOC) and network-operations center, which enable monitoring</li> </ul>	<ul style="list-style-type: none"> <li>• SOC</li> <li>• Forensics</li> <li>• Resolution teams</li> </ul>
<b>Synergies across functions</b>	<ul style="list-style-type: none"> <li>• Risk scoring of customers using common and similar customer data, such as financials, digital footprint, and nondigital records</li> </ul>	<ul style="list-style-type: none"> <li>• Risk scoring of transactions using similar analytics and common use cases based on timing, destination, source, value, frequency, device, and geolocation intelligence</li> </ul>	<ul style="list-style-type: none"> <li>• Common feedback loop to develop a holistic view on modus operandi and drive top-down use-case development</li> <li>• Pooling of resources and capabilities</li> </ul>

**1. Collaborative model**

In a collaboration model, which for most banks represents the status quo, each of the domains—financial crime, fraud, and cybersecurity—maintain their independent roles, responsibilities, and reporting. Each unit builds its own independent framework, cooperating on risk taxonomy and data and analytics for transaction monitoring, fraud, and breaches. The approach is familiar to regulators but offers banks little of the transparency needed to develop a holistic view of financial-crime risk. In addition, the collaborative model often leads to coverage gaps or overlaps among the separate groups and fails to achieve the benefits of scale that come with greater functional integration. The model’s reliance on smaller, discrete units also means banks will be less able to attract top leadership talent.

**2. Partially integrated model for cybersecurity and fraud**

Many institutions are now working toward a partial-integration model, in which cybersecurity and

fraud are partially integrated as the second line of defense. Each unit maintains independence in this model but works from a consistent framework and taxonomy, following mutually accepted rules and responsibilities. Thus a consistent architecture for prevention (such as for customer authentication) is adopted, risk-identification and assessment processes (including taxonomies) are shared, and similar interdiction processes are deployed. Deeper integral advantages, including consistency in threat monitoring and detection and lower risk of gaps and overlaps, prevail. The approach remains, however, consistent with the existing organizational structure, and little disrupts current operations. Consequently, transparency is not increased, since separate reporting is maintained. No benefits of scale accrue, and with smaller operational units still in place, the model is less attractive to top talent.

**3. Unified model**

In a fully integrated approach, the financial-crime, fraud, and cybersecurity operations are consolidated into a single framework, with common

## The three models address financial crime with progressively greater levels of operational integration.

	<b>Traditional: collaboration</b>	<b>Ongoing: partial integration<sup>1</sup></b>	<b>Future: complete integration</b>
<b>Model features</b>	<ul style="list-style-type: none"> <li>• Independent reporting, roles, and responsibilities for each type of financial crime</li> <li>• Independent framework built by each unit</li> </ul>	<ul style="list-style-type: none"> <li>• Each financial-crime unit maintains independence but uses a consistent framework and taxonomy with agreed-upon rules and responsibilities:                             <ul style="list-style-type: none"> <li>– Fraud and cybersecurity join on prevention (eg, on customer authentication)</li> <li>– Consistent processes for risk identification and assessment</li> <li>– Similar processes (eg, interdiction)</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Consolidated unit under a single framework using common assets and systems to manage risks:                             <ul style="list-style-type: none"> <li>– Single view of the customer</li> <li>– Shared analytics</li> </ul> </li> </ul>
<b>Pluses and minuses</b>	<ul style="list-style-type: none"> <li>+ Least disruptive: maintains the status quo</li> <li>+ Regulators most familiar with the model</li> <li>- Less visibility into overall financial-crime risk</li> <li>- Potential gaps/overlaps among groups</li> <li>- No scale benefits</li> <li>- Smaller units less able to attract top talent</li> </ul>	<ul style="list-style-type: none"> <li>+ More unified approach with lower risk of gaps/overlaps</li> <li>+ Organizational structure consistent with the status quo</li> <li>+ Limited disruption from current state</li> <li>- Maintains separate reporting; does not increase transparency</li> <li>- No scale benefits</li> <li>- Smaller units less able to attract top talent</li> </ul>	<ul style="list-style-type: none"> <li>+ Convergence of underlying risks</li> <li>+ Enhanced ability to attract and retain talent</li> <li>+ Standard and common framework on what is being done</li> <li>+ Benefits of scale across key roles</li> <li>- Largest organizational change</li> <li>- While converging, risks remain differentiated</li> <li>- Regulators less familiar with setup</li> </ul>



Banks have begun by closely integrating cybersecurity and fraud while stopping short of a fully integrated unit

<sup>1</sup>Mainly cybersecurity and fraud.

assets and systems used to manage risk across the enterprise. The model has a single view of the customer and shares analytics. Through risk convergence, enterprise-wide transparency on threats is enhanced, better revealing the most important underlying risks. The unified model also captures benefits of scale across key roles and thereby enhances the bank's ability to attract and retain top talent. The disadvantages of this model are that it entails significant organizational change, making bank operations less familiar to regulators. And even with the organizational change and risk convergence, risks remain differentiated.

### The imperative of integration

The integration of fraud and cybersecurity operations is an imperative step now, since the crimes themselves are already deeply interrelated. The enhanced data and analytics capabilities that integration enables are now essential tools for the prevention, detection, and mitigation of threats. Most forward-thinking institutions are working toward such integration, creating—in stages, across the domain—a more unified model based on common processes, tools, and analytics. AML activities can also be integrated, but at a slower pace, with focus on specific overlapping areas first.

The starting point for most banks has been the collaborative model, with cooperation across silos. Some banks are now shifting from this model to one that integrates cybersecurity and fraud. In the next horizon, a completely integrated model enables comprehensive treatment of cybersecurity and financial crime, including AML. By degrees, however, increased integration can improve the quality of risk management, as it enhances core effectiveness and efficiency in all channels, markets, and lines of business.

**Strategic prevention: Threats, prediction, and controls**

The idea behind strategic prevention is to predict risk rather than just react to it. To predict where





threats will appear, banks need to redesign customer and internal operations and processes based on a continuous assessment of actual cases of fraud, financial crime, and cyberthreats. A view of these is developed according to the customer journey. Controls are designed holistically, around processes rather than points. The approach can significantly improve protection of the bank and its customers (Exhibit 6).

To arrive at a realistic view of these transgressions, institutions need to think like the criminals. Crime takes advantage of a system's weak points. Current cybercrime and fraud defenses are focused on point controls or silos but are not based on an understanding of how criminals actually behave.

Exhibit 6

**With a 'customer journey' view of fraud, banks can design controls with the greatest impact.**

Potential fraud attacks in a customer journey, retail-banking example

	 <b>Open an account</b>	 <b>Change an account</b>	 <b>Make a payment</b>	 <b>Make a deposit</b>
<b>Customer-initiated actions</b>	Customer opens a new account or adds another account through online, mobile, branch, or ATM channel	Customer updates existing account (eg, adding a beneficiary or changing address)	Customer pays self or third party through wire, credit or debit card, or online transaction	Customer makes a transfer or deposit into their account
<b>Attack channel</b>				
<b>ATM</b>	<ul style="list-style-type: none"> <li>Identity theft</li> <li>Synthetic ID</li> <li>Employee-generated account</li> <li>Malware</li> </ul>	<ul style="list-style-type: none"> <li>Malware</li> </ul>	<ul style="list-style-type: none"> <li>Card skimming or trapping</li> <li>Fake PIN pad</li> <li>Cash trapping</li> <li>Shoulder surfing</li> <li>Duplicate card</li> <li>Malware</li> <li>Transaction reversal</li> </ul>	<ul style="list-style-type: none"> <li>Money laundering or terror financing</li> <li>Malware (balance multiplier)</li> </ul>
<b>Cards and e-commerce</b>		<ul style="list-style-type: none"> <li>Account takeover</li> <li>Address change</li> <li>Secondary card</li> <li>Malware</li> </ul>	<ul style="list-style-type: none"> <li>Card-not-present fraud</li> <li>Card skimming</li> <li>Malware</li> <li>Cyberattack</li> </ul>	
<b>E-banking and wire</b>		<ul style="list-style-type: none"> <li>Addition of false beneficiary</li> <li>Account takeover</li> <li>Malware</li> </ul>	<ul style="list-style-type: none"> <li>Cyberattack</li> <li>Malware</li> <li>Employee-driven transaction</li> </ul>	
<b>Branch</b>		<ul style="list-style-type: none"> <li>Account takeover</li> </ul>	<ul style="list-style-type: none"> <li>N/A</li> </ul>	

For example, if banks improve defenses around technology, crime will migrate elsewhere—to call centers, branches, or customers. By adopting this mind-set, banks will be able to trace the migratory flow of crime, looking at particular transgressions or types of crime from inception to execution and exfiltration, mapping all the possibilities. By designing controls around this principle, banks are forced to bring together disciplines (such as authentication and voice-stress analysis), which improves both efficacy and effectiveness.

#### **Efficiencies of scale and processes**

The integrated fraud and cyberrisk functions can improve threat prediction and detection while eliminating duplication of effort and resources. Roles and responsibilities can be clarified so that no gaps are left between functions or within the second line of defense as a whole. Consistent methodologies and processes (including risk taxonomy and risk identification) can be directed toward building understanding and ownership of risks. Integrating operational processes and continuously updating risk scores allow institutions to dynamically update their view on the riskiness of clients and transactions.

#### **Data, automation, and analytics**

Through integration, the antifraud potential of the bank's data, automation, and analytics can be more fully realized. By integrating the data of separate functions, both from internal and external sources, banks can enhance customer identification and verification. Artificial intelligence and machine learning can also better enable predictive analytics when supported by aggregate sources of information. Insights can be generated rapidly—to establish, for example, correlations between credential attacks, the probability of account takeovers, and criminal money movements. By overlaying such insights

onto rules-based solutions, banks can reduce the rates of false positives in detection algorithms. This lowers costs and helps investigators stay focused on actual incidents.

The aggregation of customer information that comes from the closer collaboration of the groups addressing financial crime, fraud, and cybersecurity will generally heighten the power of the institution's analytic and detection capabilities. For example, real-time risk scoring and transaction monitoring to detect transaction fraud can accordingly be deployed to greater effect. This is one of several improvements that will enhance regulatory preparedness by preventing potential regulatory breaches.

#### **The customer experience and digital trust**

The integrated approach to fraud risk can also result in an optimized customer experience. Obviously, meaningful improvements in customer satisfaction help shape customer behavior and enhance business outcomes. In the context of the risk operating model, objectives here include the segmentation of fraud and security controls according to customer experience and needs as well as the use of automation and digitization to enhance the customer journey. Survey after survey has affirmed that banks are held in high regard by their customers for performing well on fraud.

Unified risk management for fraud, financial crime, and cyberthreats thus fosters digital trust, a concept that is taking shape as a customer differentiator for banks. Security is clearly at the heart of this concept and is its most important ingredient. However, such factors as convenience, transparency, and control are also important components of digital trust. The weight customers assign to these attributes varies by segment, but very often such advantages as hassle-free authentication or the quick resolution of disputes are indispensable builders of digital trust.

## The target fraud-risk operating model: Key questions for banks

When leading banks are designing their target risk operating models for financial crime, fraud, and cybersecurity, they are probing the following questions:

- **Processes and activities:**
  - What are the key processes or activities to be conducted for customer identification and authentication, anomaly monitoring and detection, and response to risks or issues?
  - How frequently should specific activities (such as reporting) be conducted?
  - What activities can be consolidated into a “center of excellence”?
- **People and organization:**
  - Who are the relevant stakeholders in each line of defense?
  - What skills and how many people are needed to support the activities?
- What shared activities should be housed together (for example, in centers of excellence)?
- What is the optimal reporting structure for each type of financial crime—directly to the chief risk officer? To the chief operations officer? To IT?
- **Data, tools, and technologies:**
  - What data should be shared across cybersecurity, fraud, and other financial-crime divisions? Can the data sit in the same data warehouses to ensure consistency and streamlining of data activities?
  - What tools and frameworks (for example, risk-severity matrix, risk-identification rules, and taxonomy) should converge? How should they converge?
- What systems and applications do each of the divisions use? Can they be streamlined?
- **Governance:**
  - What are the governance bodies for each risk type? How do they overlap? For example, does the same committee oversee fraud and cybersecurity? Does committee membership overlap?
  - What are the specific, separate responsibilities of the first and second lines of defense?
  - What measurements are used to set the risk appetite by risk type? How are they communicated to the rest of the organization?

### A holistic view

The objective of the transformed operating model is a holistic view of the evolving landscape of financial crime. This is the necessary standpoint of efficient and effective fraud-risk management, emphasizing the importance of independent oversight and challenge through duties clearly delineated in the three lines of defense. Ultimately, institutions will have to integrate business, operations, security, and risk teams for efficient intelligence sharing and collaborative responses to threats.

### How to proceed?

When banks design their journeys toward a unified operating model for financial crime, fraud, and cybersecurity, they must probe questions about processes and activities; people and organization; data, tools, and technology; and governance (see sidebar “The target fraud-risk operating model: Key questions for banks”).

Most banks begin the journey by closely integrating their cybersecurity and fraud units. As they enhance

information sharing and coordination across silos, greater risk effectiveness and efficiency becomes possible. To achieve the target state they seek, banks are redefining organizational “lines and boxes” and, even more important, the roles, responsibilities, activities, and capabilities required across each line of defense.

Most have stopped short of fully unifying the risk functions relating to financial crime, though a few have attained a deeper integration. A leading US bank set up a holistic “center of excellence” to enable end-to-end decision making across fraud and cybersecurity. From prevention to investigation and recovery, the bank can point to significant efficiency gains. A global universal bank has gone all the way, combining all operations related to financial crime, including fraud and AML, into a single global

utility. The bank has attained a more holistic view of customer risk and reduced operating costs by approximately \$100 million.

---

As criminal transgressions in the financial-services sector become more sophisticated and break through traditional risk boundaries, banks are watching their various risk functions become more costly and less effective. Leaders are therefore rethinking their approaches to take advantage of the synergies available in integration. Ultimately, fraud, cybersecurity, and AML can be consolidated under a holistic approach based on the same data and processes. Most of the benefits are available in the near term, however, through the integration of fraud and cybersecurity operations.

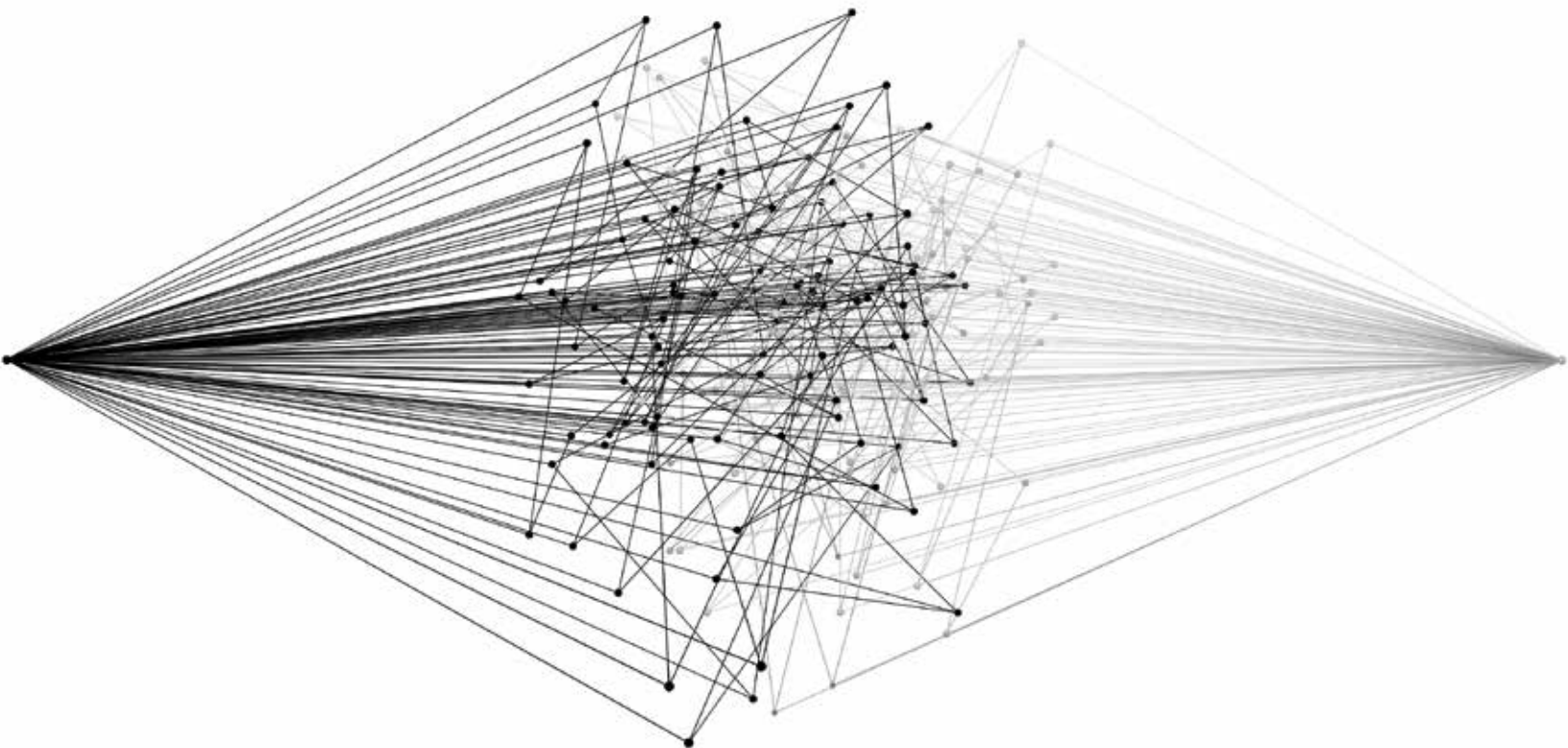
**Salim Hasham** is a partner in McKinsey’s New York office, where **Shoan Joshi** is a senior expert; **Daniel Mikkelsen** is a senior partner in the London office.

Copyright © 2019 McKinsey & Company. All rights reserved.

# Flushing out the money launderers with better customer risk-rating models

Dramatically improve detection rates by simplifying model architecture, fixing underlying data, and using machine-learning algorithms to identify high-risk behavior.

*by Daniel Mikkelsen, Azra Pravdic, and Bryan Richardson*



© Patra Kongsirimongkolchai/EyeEm/Getty Images



**Money laundering** is a serious problem for the global economy, with the sums involved variously estimated at between 2 and 5 percent of global GDP.<sup>1</sup> Financial institutions are required by regulators to help combat money laundering and have invested billions of dollars to comply. Nevertheless, the penalties these institutions incur for compliance failure continue to rise: in 2017, fines were widely reported as having totaled \$321 billion since 2008 and \$42 billion in 2016 alone.<sup>2</sup> This suggests that regulators are determined to crack down but also that criminals are becoming increasingly sophisticated.

Customer risk-rating models are one of three primary tools used by financial institutions to detect money laundering. The models deployed by most institutions today are based on an assessment of risk factors such as the customer's occupation, the customer's salary, and the banking products used. The information is collected when an account is opened, but it is infrequently updated. These inputs, along with the weight each is given, are used to calculate a risk-rating score. But the scores are notoriously inaccurate, not only failing to detect some high-risk customers but often misclassifying thousands of low-risk customers as high risk. This forces institutions to review vast numbers of cases unnecessarily, which in turn drives up their costs, annoys many low-risk customers because of the extra scrutiny, and dilutes the effectiveness of anti-money laundering (AML) efforts as resources are concentrated in the wrong place.

In the past, financial institutions have hesitated to do things differently, uncertain how regulators might respond. Yet regulators around the world are now encouraging innovative approaches to combat money laundering, and leading banks are responding by testing prototype versions of new processes and practices.<sup>3</sup> Some of those leaders have adopted the approach to customer risk rating described in this article, which integrates aspects of two other important AML tools: transaction monitoring and customer screening. The approach

identifies high-risk customers far more effectively than the method used by most financial institutions today, in some cases reducing the number of incorrectly labeled high-risk customers by between 25 and 50 percent. It also uses AML resources far more efficiently.

## **Best practice in customer risk rating**

To adopt the new generation of customer risk-rating models, financial institutions are applying five best practices. They simplify the architecture of their models, improve the quality of their data, introduce statistical analysis to complement expert judgment, continuously update customer profiles while also considering customer behavior, and deploy machine-learning and network-science tools.

### **1. Simplify the model architecture**

Most AML models are overly complex. The factors used to measure customer risk have evolved and multiplied in response to regulatory requirements and perceptions of customer risk but still are not comprehensive. Models often contain risk factors that fail to distinguish between high- and low-risk countries, for example. In addition, methodologies for assessing risk vary by line of business and model. Different risk factors might be used for different customer segments, and even when the same factor is used, it is often in name only. Different lines of business might use different occupational risk-rating scales, for instance. All this impairs the accuracy of risk scores and raises the cost of maintaining the models. Furthermore, a web of legacy and overlapping factors can make it difficult to ensure that important rules are effectively implemented. A person exposed to political risk might slip through screening processes if different business units use different checklists, for example.

Under the new approach, leading institutions examine their AML programs holistically, first aligning all models to a consistent set of risk factors, then determining the specific inputs that are relevant for each line of business (Exhibit 1). The

<sup>1</sup> "Money-laundering and globalization," UNODC, unodc.org.

<sup>2</sup> Gavin Finch, "World's biggest banks fined \$321 billion since financial crisis," Bloomberg, March 2, 2017, bloomberg.com.

<sup>3</sup> The US Treasury and banking agencies have together encouraged innovative anti-money laundering (AML) practices; see "Agencies issue a joint statement on innovative industry approaches," US Office of the Comptroller of the Currency, December 3, 2018, occ.gov. In China, the Hong Kong Monetary Authority has backed the wider use of regulatory technology, and in the United Kingdom, the financial regulator has established a fintech "sandbox" to test AML innovations.

approach not only identifies risk more effectively but does so more efficiently, as different businesses can share the investments needed to develop tools, approaches, standards, and data pipelines.

## 2. Improve data quality

Poor data quality is the single biggest contributor to the poor performance of customer risk-rating models. Incorrect know-your-customer information, missing information on company suppliers, and erroneous business descriptions impair the effectiveness of screening tools and needlessly raise the workload of investigation teams. In many institutions, more than half the cases reviewed have been labeled high risk simply due to poor data quality.

The problem can be a hard one to solve, as the source of poor data is often unclear. Any one of the systems that data pass through, including the process for collecting data, could account for the incorrect identification of occupations, for example. However, machine-learning algorithms can search exhaustively through subsegments of the data to

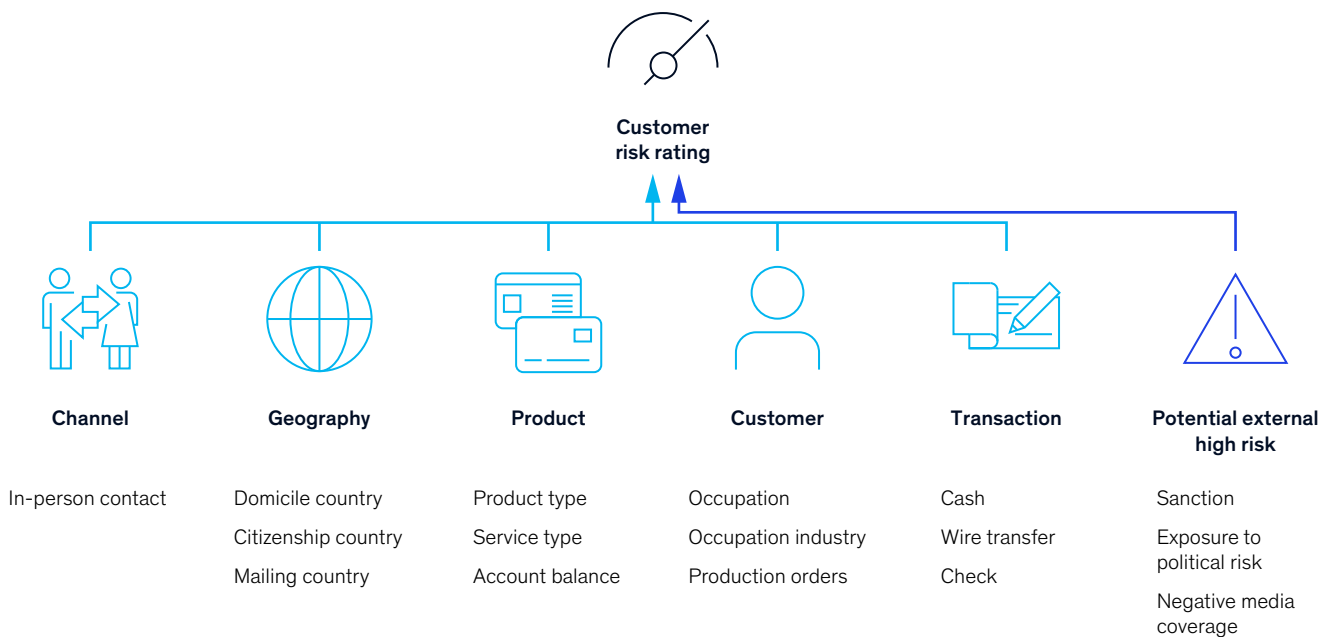
identify where quality issues are concentrated, helping investigators identify and resolve them. Sometimes, natural-language processing (NLP) can help. One bank discovered that a great many cases were flagged as high risk and had to be reviewed because customers described themselves as a “doctor” or “MD,” when the system only recognized “physician” as an occupation. NLP algorithms were used to conduct semantic analysis and quickly fix the problem, helping reduce the enhanced due-diligence backlog by more than 10 percent. In the longer term, however, better-quality data is the solution.

## 3. Complement expert judgment with statistical analysis

Financial institutions have traditionally relied on experts, as well as regulatory guidance, to identify the inputs used in risk-rating-score models and decide how to weight them. But different inputs from different experts contribute to unnecessary complexity and many bespoke rules. Moreover, because risk scores depend in large measure on

Exhibit 1

### Effective, efficient risk-rating models use a consistent set of risk factors, though inputs will vary by business line.



the experts' professional experience, checking their relevance or accuracy can be difficult. Statistically calibrated models tend to be simpler. And, importantly, they are more accurate, generating significantly fewer false-positive high-risk cases.

Building a statistically calibrated model might seem a difficult task given the limited amount of data available concerning actual money-laundering cases. In the United States, suspicious cases are passed to government authorities that will not confirm whether the customer has laundered money. But high-risk cases can be used to train a model instead. A file review by investigators can help label an appropriate number of cases—perhaps 1,000—as high or low risk based on their own risk assessment. This data set can then be used to calibrate the parameters in a model by using statistical techniques such as regression. It is critical that the sample reviewed by investigators contains enough high-risk cases and that the rating is peer-reviewed to mitigate any bias.

Experts still play an important role in model development, therefore. They are best qualified to identify the risk factors that a model requires as a starting point. And they can spot spurious inputs that might result from statistical analysis alone. However, statistical algorithms specify optimal weights for each risk factor, provide a fact base for removing inputs that are not informative, and simplify the model—for example, by removing correlated model inputs.

#### **4. Continuously update customer profiles while also considering behavior**

Most customer risk-rating models today take a static view of a customer's profile—their current residence or occupation, for example. However, the information in a profile can become quickly

outdated: most banks rely on customers to update their own information, which they do infrequently at best. A more effective risk-rating model updates customer information continuously, flagging a change of address to a high-risk country, for example. A further issue with profiles in general is that they are of limited value unless institutions are considering a person's behavior as well. We have found that simply knowing a customer's occupation or the banking products they use, for example, does not necessarily add predictive value to a model. More telling is whether the customer's transaction behavior is in line with what would be expected given a stated occupation, or how the customer uses a product.

Take checking accounts. These are regarded as a risk factor, as they are used for cash deposits. But most banking customers have a checking account. So while product risk is an important factor to consider, behavioral variables are too. Evidence shows that customers with deeper banking relationships tend to be lower risk, which means customers with a checking account as well as other products are less likely to be high risk. The number of in-person visits to a bank might also help determine more accurately whether a customer with a checking account posed a high risk, as would their transaction behavior—the number and value of cash transactions and any cross-border activity. Connecting the insights from transaction-monitoring models with customer risk-rating models can significantly improve the effectiveness of the latter.

#### **5. Deploy machine-learning and network-science tools**

While statistically calibrated risk-rating models perform better than manually calibrated ones,

**While statistically calibrated risk-rating models perform better than manually calibrated ones, machine learning and network science can further improve performance.**

machine learning and network science can further improve performance.

The list of possible model inputs is long, and many on the list are highly correlated and correspond to risk in varying degrees. Machine-learning tools can analyze all this. Feature-selection algorithms that are assumption free can review thousands of potential model inputs to help identify the most relevant features, while variable clustering can remove redundant model inputs. Predictive algorithms (decision trees and adaptive boosting, for example) can help reveal the most predictive risk factors and combined indicators of high-risk customers—perhaps those with just one product who do not pay bills but who transfer round-figure dollar sums internationally. In addition, machine-learning approaches can build competitive benchmark models to test model accuracy, and, as mentioned above, they can help fix data-quality issues.

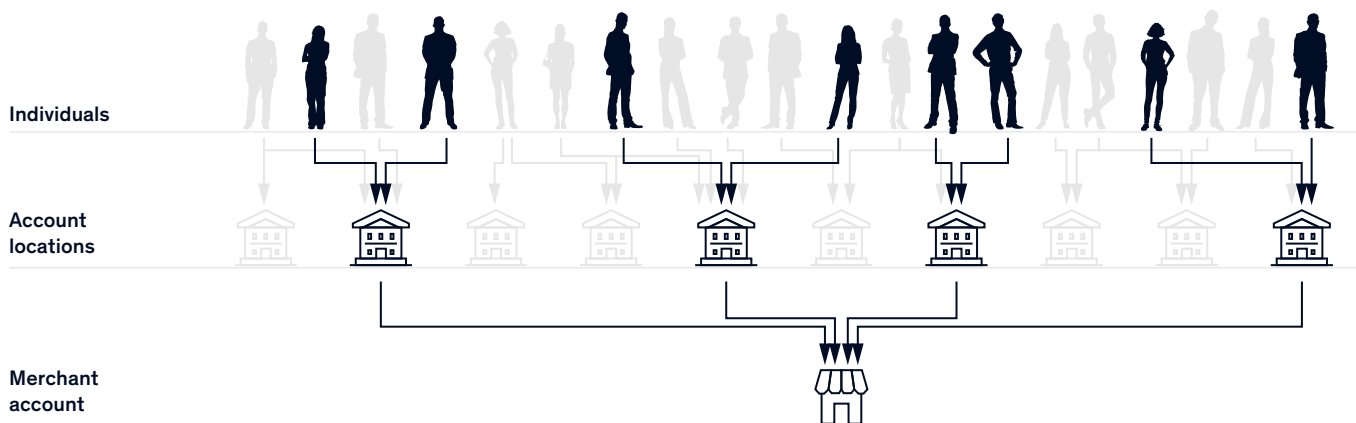
Network science is also emerging as a powerful tool. Here, internal and external data are combined

to reveal networks that, when aligned to known high-risk typologies, can be used as model inputs. For example, a bank's usual AML-monitoring process would not pick up connections among four or five accounts steadily accruing small, irregular deposits that are then wired to a merchant account for the purchase of an asset—a boat perhaps. The individual activity does not raise alarm bells. Different customers could simply be purchasing boats from the same merchant. Add in more data, however—GPS coordinates of commonly used ATMs, for instance—and the transactions start to look suspicious because of the connections between the accounts (Exhibit 2). This type of analysis could discover new, important inputs for risk-rating models. In this instance, it might be a network risk score that measures the risk of transaction structuring—that is, the regular transfer of small amounts intended to avoid transaction-monitoring thresholds.

Although such approaches can be powerful, it is important that models remain transparent. Investigators need to understand the reasoning

Exhibit 2

### Network science can reveal suspicious connections between apparently discrete accounts.



Network analytics can detect an inferred relationship based on historical patterns of co-location

behind a model's decisions and ensure it is not biased against certain groups of customers. Many institutions are experimenting with machine-based approaches combined with transparency techniques such as LIME or Shapley values that explain why the model classifies customers as high risk.

### Moving ahead

Some banks have already introduced many of the five best practices. Others have further to go. We see three horizons in the maturity of customer risk-rating models and, hence, their effectiveness and efficiency (Exhibit 3).

Most banks are in horizon one, using models that are manually calibrated and give a periodic snapshot of the customer's profile. In horizon two, statistical models use customer information that is regularly updated to rate customer risk more accurately. Horizon three is more sophisticated still.

To complement information from customers' profiles, institutions use network analytics to construct a behavioral view of how money moves around their customers' accounts. Customer risk scores are computed via machine-learning approaches utilizing transparency techniques to explain the scores and accelerate investigations. And customer data are updated continuously while external data, such as property records, are used to flag potential data-quality issues and prioritize remediation.

Financial institutions can take practical steps to start their journey toward horizon three, a process that may take anywhere from 12 to 36 months to complete (see sidebar, "The journey toward sophisticated risk-rating models").

As the modus operandi for money launderers becomes more sophisticated and their crimes

Exhibit 3

## Moving along three horizons, the model becomes more sophisticated and thus greater in its effectiveness and efficiency.



## The journey toward sophisticated risk-rating models

### Getting started: How to move from horizon one to two

Assemble a team of experts from compliance, business, data science, and technology and data.

Establish a common hierarchy of risk factors informed by regulatory guidance, experts, and risks identified in the past.

Start in bite-size chunks: pick an important model to recalibrate that the team can use to develop a repeatable process.

Assemble a file-review team to label a sample of cases as high or low risk based on their own risk assessment. Bias the sample to ensure that high-risk cases are present in sufficient numbers to train a model.

Use a fast-paced and iterative approach to cycle through model inputs quickly and identify those that align best with the overarching risk factors. Be sure there are several inputs for each factor.

Engage model risk-management and technology teams early and set up checkpoints to avoid any surprises.

### Becoming an industry leader: How to move from horizon two to three

Begin to build capabilities in machine learning, network science, and natural-language processing by hiring new experts or identifying potential internal transfers.

Construct a network view of all customers, initially building links based

on internal data and then creating inferred links. This will become a core data asset.

Set up a working group to identify technology changes that can be deployed on existing technology (classical machine learning may be easier to deploy than deep learning, for example) and those that will require longer-term planning.

Design and implement customer journeys in a way that facilitates quick updates to customer data. An in-person visit to a branch should always prompt a profile update, for example. Set up an innovation team to continuously monitor model performance and identify emerging high-risk typologies to incorporate into model calibration.

more costly, financial institutions must fight back with innovative countermeasures. Among the most effective weapons available are advanced risk-rating models. These more accurately flag suspicious actors and activities, applying machine learning and statistical analysis to better-quality data and dynamic profiles of customers and their behavior. Such models can dramatically reduce false positives and enable the concentration of resources

where they will have the greatest AML effect. Financial institutions undertaking to develop these models to maturity will need to devote the time and resources needed for an effort of one to three years, depending on each institution's starting point. However, this is a journey that most institutions and their employees will be keen to embark upon, given that it will make it harder for criminals to launder money.

**Daniel Mikkelsen** is a senior partner in McKinsey's London office, **Azra Pravidic** is an associate partner in the Brussels office, and **Bryan Richardson** is a consultant in the Vancouver office.

Copyright © 2019 McKinsey & Company. All rights reserved.

# Scotiabank's chief risk officer on the state of anti-money laundering

Daniel Moore talks about finding bad guys, creating good money, and everything in between.

*by Erez Eizenman*



**Twenty years ago**, anti–money laundering (AML) was an afterthought for most banks. Today, it's at or near the top of the executive agenda. Daniel Moore is group head and chief risk officer at Scotiabank, one of Canada's top five banks, with 99,000 employees and more than \$1 trillion in assets. Recently, McKinsey's Erez Eizenman spoke with him in Toronto about Scotiabank's efforts to combat financial crime. An edited transcript of their conversation follows.

**McKinsey:** *As chief risk officer, it's your job to stay awake at night worrying about various risks. Where does money laundering rank?*

**Daniel Moore:** I think the biggest challenge for banks these days is strategy and brand. There's a lot happening on various fronts: regulation, competition, data, and technology. And in a low-rate environment, margins are challenged. But our main concern is to understand our industry's competitive advantage, embrace it, and enhance it. One such advantage is customer trust. We have that today, and we need to value it. Customer trust derives from brand. AML, which is really about ensuring responsibility in our banking capacities, is critically important to upholding the value of brand and enhancing customer trust. So getting AML right is of critical strategic importance to our bank.

**McKinsey:** *How is the industry doing at maintaining that customer trust and managing the money-laundering risk?*

**Daniel Moore:** The industry is on the early part of that arc. Even though banking has worked at this for years, it takes a long time to move beyond regulatory compliance and into effectiveness. That's the journey the industry is on: discovering the abilities of data and technology to get to effective outcomes, as opposed to regulatory compliance. We see this in the headlines every day. We are still focused on regulatory compliance.

It's critical to understand that the landscape is changing on two frontiers. One is the regulatory frontier, and the other is the environment in which we operate. We talk often about how the bad guys change how they operate every single day. And they are as sophisticated as banks, make no mistake. But the regulatory environment is also changing. Keeping pace with both effectively isn't always easy; sometimes you need to decide which you want to pay more attention to.

**McKinsey:** *How have you managed that at Scotiabank?*

**Daniel Moore:** It's always a balancing act. There's no right answer. Knowing your regulator well, establishing a relationship, and ultimately aligning your interests are of critical importance. It's also important to have really good governance. That's something we've paid particular attention to in the last year or so. In big enterprise initiatives, it's easy to move quickly to the tactical. And the tactical becomes disorganized. So effective governance, to make sure you're focused on the right things at the right times, is important for an effective AML program.

**McKinsey:** *For many banks, managing that balance means moving beyond all the manual work required in due diligence to using technology and analytics. Was that true for you?*

**Daniel Moore:** Yes. Analytics is probably one of the most overused terms right now because it can mean so much. Analytics for AML can range from very simple, linear rules all the way to backward-propagated neural-network models. We use all of those—and everything in between—because there's yield from each one. Part of the challenge is to make sure you're using the appropriate tool at the right time for the appropriate outcome. Everyone wants to use the most sophisticated, complicated tool all the time. That isn't always the most effective



choice—nor the most explainable or acceptable from a regulatory perspective. But let's be clear: for everything from name screening to transactional monitoring, we have not found any part of our AML program that hasn't been positively and materially affected by the use of analytics.

**McKinsey:** *What are your guidelines for applying analytics to AML?*

**Daniel Moore:** The key observation is that, sometimes, effectiveness can derive from very simple outcomes, very simple rules, very simple filters. And it's important to think about where and when you apply those tools. I come back to Ajay Agrawal's paradigm of the simple economics of analytics. Analytics has made prediction very cheap, but it doesn't mitigate the need for the kind of judgment in which people review outcomes. We can modify the filters and the funnel that go into a judgment, making it more effective. We can also enhance the tools used to make a judgment more productive. But ultimately, we still need that third level of judgment in which we look at cases and outcomes. That will remain expensive. But as prediction becomes even more widely applied and cheaper, the judgment will become more productive.

**McKinsey:** *What are the technical challenges of setting up that kind of ideal, in which judgment sits atop machine models?*

**Daniel Moore:** We've had two big challenges. One is sourcing the data. Most banks deal with multiple legacy systems holding data in many places. And producing an integrated data schema from that, where you can look at data effectively, is challenging. It's not beyond the wit of man, but it's a big piece of work to get right.

The other is what we refer to as the "IP [intellectual property] of AML judgment." It is knowing what you're solving for. Many of today's high-profile

cases would have been compliant with yesterday's rules. So knowing about regulatory change, knowing what to look for in your systems to produce effective outcomes, is critically important. That's an ongoing education.

**McKinsey:** *We'd love to understand what you think about the future of analytics in AML.*

**Daniel Moore:** The challenge is that we're not only looking for a needle in a haystack, we're looking for a needle in a stack of needles. And we don't even know if we have the whole stack of needles when we're doing it. So in the future, collaboration will be vital: across the financial-services industry, government, and law enforcement. The ability to put together our data sets and collaborate on typologies of attack—and the use of both advanced-encryption methods and analytics methods to mine the data—will enhance yields by orders of magnitude. That's the ultimate direction. Some jurisdictions are further ahead than others. But I think all are moving in this direction. And ultimately, that comprehensive, 360-degree view will produce better outcomes for all stakeholders.

**McKinsey:** *Let's talk about the regulatory side of the balance you mentioned. Explaining your new uses of analytics could be a difficult conversation to have with a regulator.*

**Daniel Moore:** Ultimately, it's about understanding that the regulator's objectives are aligned with our objectives. Simply put, that's to find bad guys inside our system. We both want to achieve the same thing. So how do we enhance that alignment of interests? Communication and relationships are important in whatever jurisdiction you're operating in—relationships with the regulator, bringing them along on the journey. In many jurisdictions, including the US, we've seen a shift in regulatory expectations where they are more open to a focus on the use of analytics to produce better outcomes.

**McKinsey:** *Have you educated the regulator as you go?*

**Daniel Moore:** It behooves us as an industry, because we are at the “coal face” of analytics, to educate the regulator. We’ve also found that the regulators are highly interested in learning and taking this journey alongside us. And that makes for effective challenge and governance on what we produce.

**McKinsey:** *How do you think about metrics and tracking, both internally and to share with the regulator?*

**Daniel Moore:** Like any big initiative, there are several metrics that can help, starting with production metrics in AML operations. In technology, we look at effectiveness, efficiency, and coverage metrics. We also have KPIs [key performance indicators] for a wide variety of outputs and backlogs. But ultimately, coming back to our objective, what it comes down to is risk appetite and our key risk indicators [KRIs]. Are we making progress against our risk-appetite metrics? Every form of risk, including AML, should have KRIs to assess the inherent risk, the mitigators, and the residual risk.

**McKinsey:** *Big transformations need metrics and people to keep them on track. How critical is talent as part of that equation?*

**Daniel Moore:** It’s probably obvious that talent is critical to the outcome. But talent isn’t just smart people. We have lots of smart people. Talent means people who have been on this journey and know the common pitfalls and can help you avoid them. The industry has been working on AML for many years now, so talent is available.

Some of those pitfalls are in data science. Historically, it’s been difficult to find data scientists. But the supply is increasing as universities and other organizations and even industry are training more people. The real challenge is finding people who understand both the data science and the business need. That’s pure gold—and rare.

**McKinsey:** *Once you find the right people, how do you set them up to be successful?*

**Daniel Moore:** That’s really a question of organizational alignment or culture. When a data scientist meets with a business partner, will they find engagement or resistance? And the question then is, how important is AML to an organization? Because we see AML as intrinsically linked to brand, we believe it’s of fundamental importance to the organization.

**McKinsey:** *No matter how large your AML team grows to be, there’s always a requirement for AML*

**“The real challenge is finding people who understand both the data science and the business need. That’s pure gold—and rare.”**

*to be truly owned by the front line. How do you both educate the front line and instill in them that sense of ownership?*

**Daniel Moore:** Many organizations, and we are not immune, start big risk initiatives within the risk group. And maybe that's an OK place to start. But you'll never be long-term successful if the risk is not owned by the first line of defense. It's important to create accountability, so the first line feels like it owns—and does in fact own—the risk. Governance, challenge, and oversight come from the second line.

It's an important point that cannot be underscored enough. We need to know our customers and understand that the capacities we've created, which are extraordinary and highly efficient and highly tuned, are used for the betterment of society, its communities, and its individuals. We call that “good money,” and we make sure that good money is what flows over our counters every single day.

**McKinsey:** *How has that concept resonated in your bank?*

**Daniel Moore:** If you asked me ten years ago, when I was in wholesale banking, whether I would be excited about being involved in AML, the answer would have been a resounding “no.” It was a paper exercise. It was a compliance exercise. But when you shift your perspective and realize that every bank today is faced with people who want to exploit it to conduct criminal enterprises, terrorism, human trafficking, you know that's not the sort of bank—or the sort of industry—that you want to be part of. When you make it real in that way, people wake up and realize, “We are not going to walk by that standard.” Because the standard that you walk by is a standard that you accept.

**McKinsey:** *That's a compelling change story. Our research shows that the number-one reason a transformation fails is that the top-leadership*

*team doesn't offer a convincing story of why change is needed.<sup>1</sup> How important has that story been for Scotiabank?*

**Daniel Moore:** The board, the CEO, the operating committee—they are all highly engaged on our AML journey and understand its importance to the bank, why it matters for us to be responsible bankers, and why it matters to the commercial enterprise.

**McKinsey:** *What did you do to ensure that everyone in the bank heard that tone from the top?*

**Daniel Moore:** There's no one silver bullet. It's like any other cultural change. It will take time. And it requires a variety of modalities to get it right: regular memoranda, emails, frequent mentions in town halls. Any forum where you can mention at least seven times the importance of what you're after will bring that message home. We made some powerful videos that resonated throughout the organization. We brought in victims of human trafficking to speak to our bankers to help them understand what this means and how this is happening in our own backyard. Human trafficking is the fastest-growing form of crime in AML today. It's a real tragedy in the cities in which we operate. It's a stark message. But once you get it out there, people really lean into the outcome.

The communications make it real, moving it off the piece of paper with the checklist and into the “why” of what we're doing. That's true also of the regulatory direction in which we're heading and the way we operate inside the bank. Simon Sinek talks about starting with “why.” That's the core of what we do. And landing that is of critical importance.

**McKinsey:** *What role does the board play in this?*

**Daniel Moore:** AML is a significant expenditure of calories. It takes a lot of investment to get it right. You absolutely need the board's high-level engagement, as we've had, to make sure you're

---

<sup>1</sup> “Why transformations fail: A conversation with Seth Goldstrom,” February 2019, McKinsey.com.

focused on getting it right and that you have the resources available to deploy against that outcome.

**McKinsey:** *Do you view AML as a source of competitive advantage?*

**Daniel Moore:** Yes. An effective AML program will be a competitive advantage, not simply because of what it does to enhance the brand and build trust, but also because it allows you to do what you do more effectively. The consequences of getting it wrong are vast. A bank that falls down on AML might lose 20,000 commercial customers in a month. That's because environmental, social, and governance issues matter more today than ever.

But the core of AML is relationships: knowing your customers better and being able to take smart risks of every kind when the bank underwrites a customer. Banks have a charter and a mandate in the communities and societies in which they operate to create capital for those that will put it to responsible uses.

Understanding our customers better, a better ability to rate risks, and intelligence about where we're deploying our capital will allow the industry to responsibly deploy capital with those that need it, which is valuable to the communities in which we operate and to the banks that are able to operate safely in those jurisdictions. That's what we're working on.

**Erez Eizenman** is a partner in McKinsey's Toronto office. **Daniel Moore** is group head and chief risk officer at Scotiabank.

Copyright © 2019 McKinsey & Company. All rights reserved.

# The risk-based approach to cybersecurity

The most sophisticated institutions are moving from a maturity-based to a risk-based approach for managing cyberrisk. Here is how they are doing it.

*by Jim Boehm, Nick Curcio, Peter Merrath, Lucy Shenton, and Tobias Stähle*



© Ivcandy/Getty Images

**Top managers at most companies** recognize cyberrisk as an essential topic on their agendas. Worldwide, boards and executive leaders want to know how well cyberrisk is being managed in their organizations. In more advanced regions and sectors, leaders demand, given years of significant cybersecurity investment, that programs also prove their value in risk-reducing terms. Regulators are challenging the levels of enterprise resilience that companies claim to have attained. And nearly everyone—business executives, regulators, customers, and the general public—agree that cyberrisk is serious and calls for constant attention (Exhibit 1).

What, exactly, organizations should do is a more difficult question. This article is advancing a risk-based approach to cybersecurity, which means that to decrease enterprise risk, leaders must identify and focus on the elements of cyberrisk to target. More specifically, the many components of cyberrisk must be understood and prioritized for enterprise cybersecurity efforts. While this approach to cybersecurity is complex, best practices for achieving it are emerging.

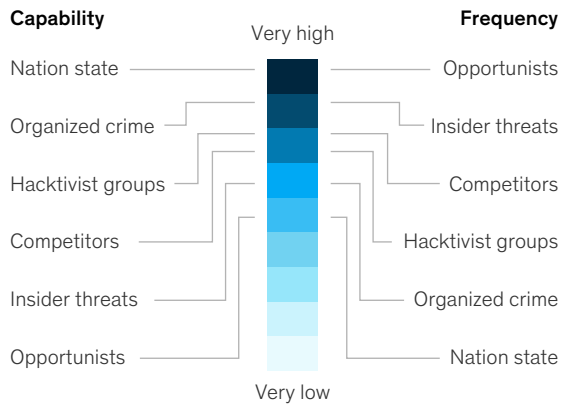
To understand the approach, a few definitions are in order. First, our perspective is that cyberrisk is *only* another kind of operational risk. That is, “cyberrisk” refers to the potential for business losses of all kinds—financial, reputational, operational, productivity related, and regulatory related—in the digital domain. Cyberrisk can also cause losses in the physical domain, such as damage to operational equipment. But it is important to stress that cyberrisk is a form of business risk.

Furthermore, cyberrisks are not the same as cyberthreats, which are the particular dangers that create the potential for cyberrisk. Threats include privilege escalation, vulnerability exploitation, or phishing.<sup>1</sup> Cyberthreats exist in the context of

Exhibit 1

## Cyberthreats are growing in severity and frequency.

**Cyberthreat capacity and frequency today, threat actor**



enterprise cyberrisk as potential avenues for loss of confidentiality, integrity, and availability of digital assets. By extension, the risk impact of cyberthreats includes fraud, financial crime, data loss, or loss of system availability.

Decisions about how best to reduce cyberrisk can be contentious. Taking into account the overall context in which the enterprise operates, leaders must decide which efforts to prioritize: Which projects could most reduce enterprise risk? What methodology should be used to make clear to enterprise stakeholders (especially in IT) that those priorities will have the greatest risk-reducing impact for the enterprise? That clarity is crucial in organizing and executing those cyber projects in a focused way.

At the moment, attackers benefit from organizational indecision on cyberrisk—including the prevailing lack of clarity about the danger

<sup>1</sup> Privilege escalation is the exploitation of a flaw in a system for the purpose of gaining unauthorized access to protected resources. Vulnerability exploitation is an attack that uses detected vulnerabilities to exploit (surreptitiously utilize or damage) the host system.

and failure to execute effective cyber controls. Debilitating attacks on high-profile institutions are proliferating globally, and enterprise-wide cyber efforts are needed now with great urgency. It is widely understood that there is no time to waste: business leaders everywhere, at institutions of all sizes and in all industries, are earnestly searching for the optimal means to improve cyber resilience. We believe we have found a way to help.

### **The maturity-based cybersecurity approach: A dog that's had its day**

Even today, maturity-based approaches to managing cyberrisk are still the norm. These approaches focus on achieving a particular level of maturity by building certain capabilities. To achieve the desired level, for example, an organization might build a security-operations center to improve the maturity of assessing, monitoring, and responding to potential threats to enterprise information systems and applications. Or it might implement multifactor authentication (MFA) across the estate to improve maturity of access control. A maturity-based approach can still be helpful in some situations—for example, to get a program up and running from scratch at an enterprise that is so far behind it has to “build everything.” For institutions that have progressed even a step beyond that, however, a maturity-based approach is inadequate. It can never be more than a proxy for actually measuring, managing, and reducing enterprise risk.

A further issue is that maturity-based programs, as they grow organically, tend to stimulate unmanageable growth of control and oversight. In monitoring, for example, a maturity-based program will tend to run rampant, aspiring to “monitor everything.” Before long, the number of applications queued to be monitored across the enterprise will outstrip the capacity of analysts to monitor them, and the installation of monitors will bog

down application-development teams. The reality is that some applications represent more serious vulnerabilities—and therefore greater potential for risk—than others. To focus directly on risk reduction, organizations need to figure out how to move from a stance of monitoring everything to one in which particular applications with high risk potential are monitored in particular ways.

Another issue related to the monitor-everything stance is inefficient spending. Controls grow year after year as program planning for cybersecurity continues to demand more spending for more controls. But is enterprise risk being reduced? Often the right answers lie elsewhere—for example, the best return on investment in enterprise-risk reduction is often in employee awareness and training. Yet a maturity-based model does not call for the organization to gather enough information to know that it should divert the funding needed for this from additional application monitoring. Spending on both will be expected, though the one effort (awareness and training) may have a disproportionate impact on enterprise-risk reduction relative to the other.

If the objective is to reduce enterprise risk, then the efforts with the best return on investment in risk reduction should draw the most resources. This approach holds true across the full control landscape, not only for monitoring, but also for privileged-access management, data-loss prevention (DLP), and so forth. All of these capabilities reduce risk somewhat and somehow, but most companies are unable to determine exactly how and by how much.

The final (and most practical) drawback of maturity-based programs is that they can create paralyzing implementation gridlock. The few teams or team members capable of performing the hands-on implementation work for the many controls needed

become overloaded with demand. Their highly valuable attention is split across too many efforts. The frequent result is that no project is ever fully implemented, so program dashboards show perpetual “yellow” status for the full suite of cyber initiatives.

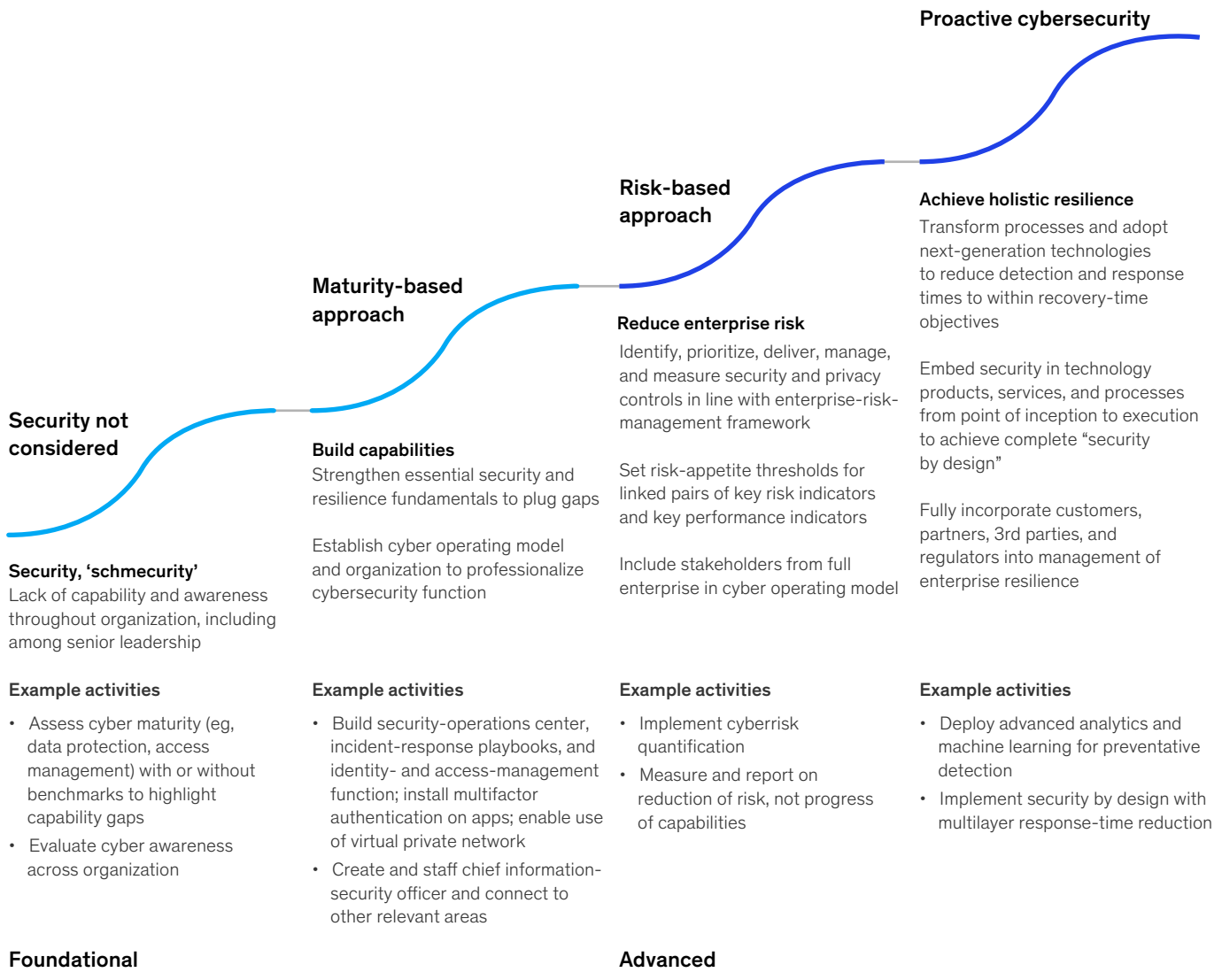
The truth is that in today’s hyperconnected world, maturity-based cybersecurity programs are no longer adequate for combating cyberrisks. A more strategic, risk-based approach is imperative for effective and efficient risk management (Exhibit 2).

## Reducing risk to target appetite at less cost

The risk-based approach does two critical things at once. First, it designates risk reduction as the primary goal. This enables the organization to prioritize investment—including in implementation-related problem solving—based squarely on a cyber program’s effectiveness in reducing risk. Second, the program distills top management’s risk-reduction targets into precise, pragmatic implementation programs with clear alignment from the board to the front line. Following the risk-

Exhibit 2

**For many companies, the risk-based approach is the next stage in their cybersecurity journey.**





based approach, a company will no longer “build the control everywhere”; rather, the focus will be on building the appropriate controls for the worst vulnerabilities, to defeat the most significant threats—those that target the business’s most critical areas. The approach allows for both strategic and pragmatic activities to reduce cyberrisks (Exhibit 3).

Companies have used the risk-based approach to effectively reduce risk and reach their target risk appetite at significantly less cost. For example, one company, by simply reordering the security initiatives in its backlog according to the risk-based approach, increased its projected risk

reduction 7.5 times above the original program at no added cost. Another company discovered that it had massively overinvested in controlling new software-development capabilities as part of an agile transformation. The excess spending was deemed necessary to fulfill a promise to the board to reach a certain level of maturity that was, in the end, arbitrary. Using the risk-based approach, the company scaled back controls and spending in areas where desired digital capabilities were being heavily controlled for no risk-reducing reason. A particular region of success with the risk-based approach has been Latin America, where a number of companies have used it to leapfrog a generation of maturity-based thinking (and spending). Instead

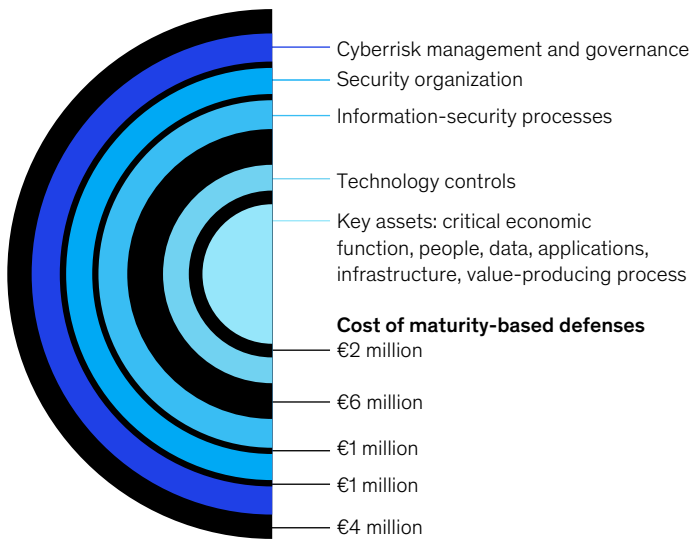
Exhibit 3

**A risk-based approach builds customized controls for a company’s critical vulnerabilities to defeat attacks at lower overall cost.**

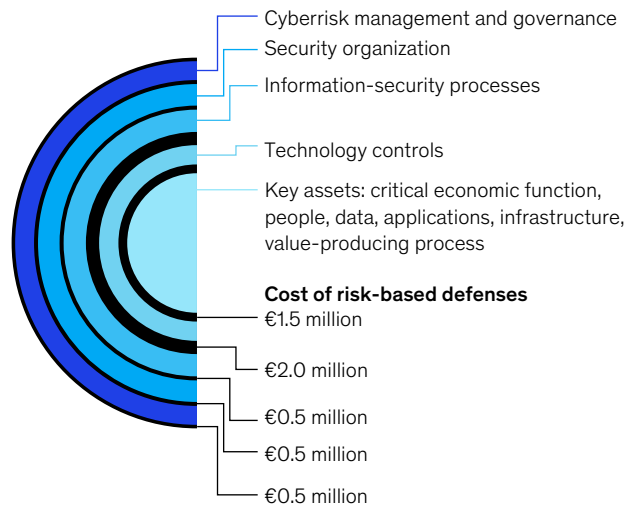
**Maturity-based versus risk-based cybersecurity**

**Maturity-based approach:** builds highest level of defense around everything

**Risk-based approach:** optimizes defensive layers for risk reduction and cost; critical assets are highly protected, but at less expense and in ways that improve productivity



Total cost  
**€14 million**



Total cost  
**€5 million**

Note: Costs are illustrative but extrapolated from real-world examples and estimates.

of recapitulating past inefficiencies, these companies are able to build exactly what they need to reduce risk in the most important areas, right from the start of their cybersecurity programs. Cyberattackers are growing in number and strength, constantly developing destructive new stratagems. The organizations they are targeting must respond urgently but also seek to reduce risk smartly, in a world of limited resources.

### **A transformation in sequential actions**

Companies adopting the risk-based approach and transforming their “run” and “change” activities accordingly inevitably face the crucible of how to move from maturity-based to risk-based cybersecurity. From the experience of several leading institutions, a set of best-practice actions has emerged as the fastest path to achieving this transformation. These eight actions taken roughly in sequence will align the organization toward the new approach and enable the appropriate efforts to reduce enterprise risk:

1. Fully embed cybersecurity in the enterprise-risk-management framework.
2. Define the sources of enterprise value across teams, processes, and technologies.
3. Understand the organization’s enterprise-wide vulnerabilities—among people, processes, and technology—internally and for third parties.
4. Understand the relevant “threat actors,” their capabilities, and their intent.
5. Link the controls in run activities and change programs to the vulnerabilities that they address and determine what new efforts are needed.
6. Map the enterprise risks from the enterprise-risk-management framework, accounting for the threat actors and their capabilities, the enterprise vulnerabilities they seek to exploit, and the security controls of the organization’s cybersecurity run activities and change program.

7. Plot risks against the enterprise-risk appetite and report on how cyber efforts have reduced enterprise risk.
8. Monitor risks and cyber efforts against risk appetite, key risk indicators (KRIs), and key performance indicators (KPIs).

#### **1. Fully embed cybersecurity in the enterprise-risk-management framework**

A risk-based cyber program must be fully embedded in the enterprise-risk-management framework. The framework should not be used as a general guideline but rather as the organizing principle. In other words, the risks the enterprise faces in the digital domain should be analyzed and categorized into a cyberrisk framework. This approach demystifies cyberrisk management and roots it in the language, structure, and expectations of enterprise-risk management. Once cyberrisk is understood more clearly as business risk that happens in the digital domain, the organization will be rightly oriented to begin implementing the risk-based approach.

#### **2. Define the sources of enterprise value**

An organization’s most valuable business work flows often generate its most significant risks. It is therefore of prime importance to identify these work flows and the risks to which they are susceptible. For instance, in financial services, a loan process is part of a value-creating work flow; it is also vulnerable to data leakage, an enterprise risk. A payment process likewise creates value but is susceptible to fraud, another enterprise risk. To understand enterprise risks, organizations need to think about the potential impact on their sources of value.

Identifying the sources of value is a fairly straightforward exercise, since business owners will have already identified the risks to their business. Cybersecurity professionals should ask the businesses about the processes they regard as valuable and the risks that they most worry about.

Making this connection between the cybersecurity team and the businesses is a highly valuable step in itself. It motivates the businesses to care more deeply about security, appreciating the bottom-line impact of a recommended control. The approach is far more compelling than the maturity-based approach, in which the cybersecurity function peremptorily informs the business that it is implementing a control “to achieve a maturity of 3.0.”

The constituents of each process—relevant teams, critical information assets (“crown jewels”), the third parties that interact with the process, and the technology components on which it runs—can be defined, and the vulnerabilities to those constituent parts can be specified.

### **3. Understand vulnerabilities across the enterprise**

Every organization scans its infrastructure, applications, and even culture for vulnerabilities, which can be found in areas such as configuration, code syntax, or frontline awareness and training. The vulnerabilities that matter most are those connected to a value source that particular threat actors with relevant capabilities can (or intend to) exploit. The connection to a source of value can be direct or indirect. A system otherwise rated as having low potential for a direct attack, for example, might be prone to lateral movement—a method used by attackers to move through systems seeking the data and assets they are ultimately targeting.

Once the organization has plotted the people, actions, technology, and third-party components of its value-creating processes, then a thorough identification of associated vulnerabilities can proceed. A process runs on a certain type of server, for example, that uses a certain operating system (OS). The particular server–OS combination will have a set of identified common vulnerabilities and exposures. The same will be true for storage, network, and end-point components. People, process, and third-party vulnerabilities can be determined by similar methodologies.

Of note, vulnerabilities and (effective) controls exist in a kind of reverse symbiosis: where one is present, the other is not. Where sufficient control is present, the vulnerability is neutralized; without the control, the vulnerability persists. Thus, the enterprise’s vulnerabilities are most practically organized according to the enterprise-approved control framework.<sup>2</sup> Here synergies begin to emerge. Using a common framework and language, the security, risk, IT, and frontline teams can work together to identify what needs to be done to close vulnerabilities, guide implementation, and report on improvements in exactly the same manner and language. Experience confirms that when the entire organization shares a common way of thinking about vulnerabilities, security can be significantly enhanced.

---

<sup>2</sup> This can include the National Institute of Standards and Technology (NIST) Cybersecurity Framework, NIST National Vulnerability Database (NIST special publication 800-53), ISO 27001 and 27002 (standards for information-security-management systems), and Federal Financial Institutions Examination Council Cybersecurity Assessment Tool.

**Experience confirms that when the entire organization shares a common way of thinking about vulnerabilities, security can be significantly enhanced.**

#### **4. Understand relevant threat actors and their capabilities**

The groups or individuals an organization must worry about—the threat actors—are determined by how well that organization's assets fit with the attackers' goals—economic, political, or otherwise. Threat actors and their capabilities—the tactics, techniques, and procedures they use to exploit enterprise security—define the organization's threat landscape.

Only by understanding the specific threat landscape can an organization reduce risk. Controls are implemented according to the most significant threats. Threat analysis begins with the questions: Which threat actors are trying to harm the organization, and what are they capable of? In response, organizations can visualize the vulnerabilities commonly exploited by relevant threats, and appropriate controls can then be selected and applied to mitigate these specific vulnerability areas.

In identifying the controls needed to close specific gaps, organizations need to size up potential attackers, their capabilities, and their intentions—the threat actors' strength and will (intention) to create a risk event. This involves collecting information on and understanding how the attackers connect, technically and nontechnically, to the people, process, and technology vulnerabilities within the enterprise.

#### **5. Address vulnerabilities**

To defeat threat actors, vulnerabilities discovered in action three either will be closed by existing controls—normal run activities or existing change initiatives—or will require new control efforts. For existing controls, the cyber-governance team (for run) and the program-management team (for change) map their current activities to the same control framework used to categorize vulnerabilities. This will show the controls already in place and those in development. Any new controls needed are added to the program backlog as either stand-alone or composite initiatives.

While an organization may not be able to complete all initiatives in the backlog in a single year, it will now be able to choose what to implement from the full spectrum of necessary controls relevant to the enterprise because they are applicable for frustrating relevant threat capabilities. The risk-based approach importantly bases the scope of both existing and new initiatives in the same control framework. This enables an additional level of alignment among teams: delivery teams charged with pushing and reporting on initiative progress can finally work efficiently with the second and third lines of defense (where relevant), which independently challenge control effectiveness and compliance. When the program-delivery team (acting as the first line of defense) sits down with the second and third lines, they will all be speaking the same language and using the same frameworks. This means that the combined groups can discuss what is and is not working, and what should be done.

#### **6. Map the enterprise-risk ecosystem**

A map of enterprise risks—from the enterprise-risk-management framework to enterprise vulnerabilities and controls to threat actors and their capabilities—makes visible a “golden thread,” from control implementation to enterprise-risk reduction. Here the risk-based approach can begin to take shape, improving both efficiency in the application of controls and the effectiveness of those controls in reducing risks.

Having completed actions one through five, the organization is now in a position to build the risk-based cybersecurity model. The analysis proceeds by matching controls to the vulnerabilities they close, the threats they defeat, and the value-creating processes they protect. The run and change programs can now be optimized according to the current threat landscape, present vulnerabilities, and existing program of controls. Optimization here means obtaining the greatest amount of risk reduction for a given level of spending. A desired level of risk can be “priced” according to the

initiatives needed to achieve it, or the entry point for analysis can be a fixed budget, which is then structured to achieve the greatest reduction in risk.

Cybersecurity optimization determines the right level and allocation of spending. Enterprise-risk reduction is directly linked to existing initiatives and the initiation of new ones. The analysis develops the fact base needed for tactical discussions on overly controlled areas whence the organization might pull back as well as areas where better control for value is needed.

By incorporating all components in a model and using the sources of value and control frameworks as a common language, the business, IT, risk, and cybersecurity groups can align. Discussions are framed by applying the enterprise control framework to the highest sources of value. This creates the golden-thread effect. Enterprise leadership (such as the board and the risk function)

can identify an enterprise risk (such as data leakage), and the cybersecurity team can report on what is being done about it (such as a DLP control on technology or a social-engineering control on a specific team). Each part is connected to the other, and every stakeholder along the way can connect to the conversation. The model is at the center, acting both as a translator and as an optimizer. The entire enterprise team, from the board to the front line, knows what to do and can move in a unified way to do it.

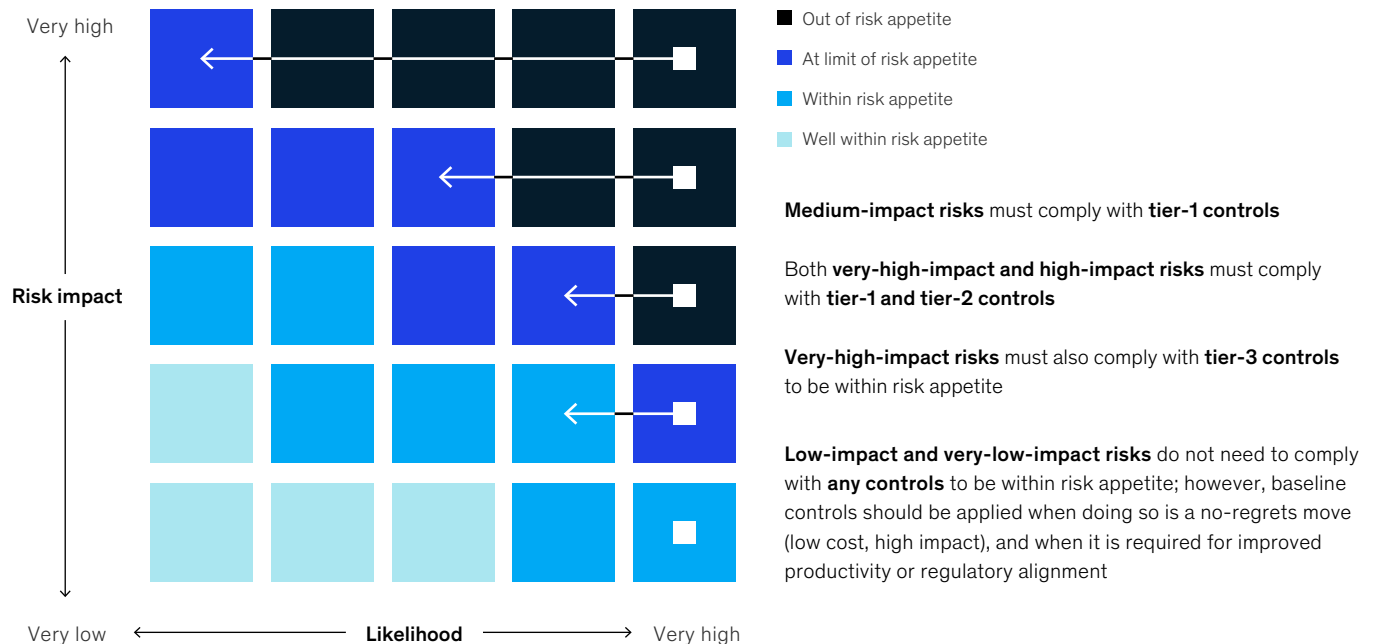
### 7. Plot risks against risk appetite and report on risk reduction

Once the organization has established a clear understanding of and approach to managing cyberrisk, it can ensure that these concepts are easily visualized and communicated to all stakeholders. This is done through a risk grid, where the application of controls is sized to the potential level of risk (Exhibit 4).

Exhibit 4

## The risk-based approach applies controls according to the risk appetite and the likelihood and potential impact of a risk event.

### Risk events by size of impact and likelihood of occurrence



The assumption in this use of the classic risk grid is that the enterprise-risk appetite has been defined for each enterprise risk. The potential impact for each enterprise-risk scenario can then be plotted on the risk grid. Once the relationships among the threats, vulnerabilities, and applied controls are modeled and understood, the risks can be evaluated according to their likelihood. As more controls are applied, the risk levels are reduced to the risk appetite. This is the way the cyber program can demonstrate impact in terms of enterprise-risk reduction.

As new threats emerge, new vulnerabilities will become apparent. Existing controls may become ineffective, and enterprise risks can move in the opposite direction—even to the point where risk-appetite limits are exceeded. For information-security-management systems, the risk grid allows stakeholders to visualize the dynamic relationships among risks, threats, vulnerabilities, and controls and react strategically, reducing enterprise risks to the appropriate risk-appetite level.

## **8. Monitor risks and cyber efforts using risk appetite and key risk and performance indicators**

At this point, the organization's enterprise-risk posture and threat landscape are understood, and the risk-based cybersecurity program is in place. The final step is to monitor and manage for success.

Many companies attempt to measure cyber maturity according to program completion rather than by actual reduction of risk. If a security function reports that the DLP program is 30 percent delivered, for example, the enterprise assumption is that risk of data leakage is 30 percent reduced. If an MFA initiative is 90 percent implemented, the assumption is that the risk of unauthorized access is almost eliminated. These assumptions are false, however, because actual risk-reducing results are not being measured in these examples.

## **Linking a key risk indicator to a key performance indicator**

**A data-loss-prevention (DLP)** program is a helpful control to reduce the enterprise risk of data leakage. The critical assets identified by the enterprise-risk-management function as requiring DLP coverage can become the output metric, or key risk indicator (KRI). Assuming that the KRI is not 100 percent, then the linked input metric, or key performance indicator (KPI),

could be the proportion of critical assets covered since the last reporting period versus the total expected to be covered. Enterprise leaders will see these two metrics on the reporting dashboard. They can then assess the progress toward the appetite-linked thresholds and with delivery teams discuss what, if anything, is needed to continue meeting (or possibly exceeding) expectations.

With KRIs and KPIs systematically incorporated into a digital dashboard, executives have complete risk-based measurement and reporting at their fingertips. They can actively participate in risk-reduction efforts—influencing their progress, projections, performance, and achievement of risk thresholds.

Metrics need to measure both inputs and outputs; inputs, in this case, are risk-reduction efforts undertaken by the enterprise, while the output is the actual reduction in enterprise risk. The input metric here is a KPI: measuring the performance of a program or a run function. The output metric is really a KRI: measuring the risk level associated with a potential risk scenario. The thresholds for the KRIs must be tied directly to risk-appetite levels (the KPI thresholds can also be linked in this way). For example, if risk appetite for data leakage is zero, then the systemic controls (and corresponding “red” thresholds) must be higher than they would be if a certain percentage of leakage is allowed over a certain period. Of course, tolerances for cyberincidents may not always be set at zero. In most cases, it is impossible to stop all cyberattacks, so sometimes controls can be developed that tolerate some incidents.

One way to think about KRIs and KPIs is with regard to the relationship between altitude and trajectory. A KRI gives the current risk level of the enterprise (the “risk altitude”), while a KPI indicates the direction toward or away from the enterprise-risk-appetite level (“risk trajectory”). An enterprise may not yet have arrived at the leadership’s KRI target, but a strong KPI trajectory would suggest that it will soon. Conversely, an enterprise may have hit the desired KRI threshold, but the KPIs of the run activity may be backsliding and give cause for concern.

Executives are often forced to make sense of a long list of sometimes conflicting metrics. By linking KRIs

and KPIs, the cybersecurity team gives executives the ability to engage in meaningful problem-solving discussions on which risks are within tolerances, which are not, and why (see sidebar, “Linking a key risk indicator to a key performance indicator”).

The risk-based approach to cybersecurity is thus ultimately interactive—a dynamic tool to support strategic decision making. Focused on business value, utilizing a common language among the interested parties, and directly linking enterprise risks to controls, the approach helps translate executive decisions about risk reduction into control implementation. The power of the risk-based approach to optimize for risk reduction at any level of investment is enhanced by its flexibility, as it can adjust to an evolving risk-appetite strategy as needed.

---

Many leading companies have a cyber-maturity assessment somewhere in their archives; some still execute their programs to achieve certain levels of maturity. The most sophisticated companies are, however, moving away from the maturity-based cybersecurity model in favor of the risk-based approach. This is because the new approach allows them to apply the right level of control to the relevant areas of potential risk. For senior leaders, boards, and regulators, this means more economical and effective enterprise-risk management.

**Jim Boehm** is an associate partner in McKinsey’s Washington, DC, office; **Nick Curcio** is a cyber solutions analyst in the New York office; **Peter Merrath** is an associate partner in the Frankfurt office, where **Tobias Stähle** is a consultant; and **Lucy Shenton** is a cyber solutions specialist in the Berlin office.

The authors wish to thank Rich Isenberg for his contributions to this article.

Copyright © 2019 McKinsey & Company. All rights reserved.

# Cybersecurity: Linchpin of the digital enterprise

As companies digitize businesses and automate operations, cyber risks proliferate. Here is how a cybersecurity organization can support a secure digital agenda.

*by James M. Kaplan, Wolf Richter, and David Ware*



© Chad Baker/Getty Images



**Two consistent and related themes** in enterprise technology have emerged in recent years, both involving rapid and dramatic change. One is the rise of the digital enterprise across sectors and internationally. The second is the need for IT to react quickly and develop innovations aggressively to meet the enterprise's digital aspirations. Exhibit 1 presents a "digitization index"—the results of research on the progress of enterprise digitization within companies, encompassing sectors, assets, and operations.

As IT organizations seek to digitize, however, many face significant cybersecurity challenges. At company after company, fundamental tensions arise between the business's need to digitize and the cybersecurity team's responsibility to protect the organization, its employees, and its customers within existing cyber operating models and practices.

If cybersecurity teams are to avoid becoming barriers to digitization and instead become its enablers, they must transform their capabilities along three dimensions. They must improve risk management, applying quantitative risk analytics. They must build cybersecurity directly into businesses' value chains. And they must support the next generation of enterprise-technology platforms, which include innovations like agile development, robotics, and cloud-based operating models.

### **Cybersecurity's role in digitization**

Every aspect of the digital enterprise has important cybersecurity implications. Here are just a few examples. As companies seek to create more digital customer experiences, they need to determine how to align their teams that manage fraud prevention, security, and product development so they can design controls, such as authentication, and create experiences that are both convenient and secure. As companies adopt massive data analytics, they must determine how to identify risks created by data sets that integrate many types of incredibly sensitive customer information. They must also

incorporate security controls into analytics solutions that may not use a formal software-development methodology. As companies apply robotic process automation (RPA), they must manage bot credentials effectively and make sure that "boundary cases"—cases with unexpected or unusual factors, or inputs that are outside normal limits—do not introduce security risks.

Likewise, as companies build application programming interfaces (APIs) for external customers, they must determine how to identify vulnerabilities created by interactions between many APIs and services, and they must build and enforce standards for appropriate developer access.<sup>1</sup> They must continue to maintain rigor in application security as they transition from waterfall to agile application development.

### **Challenges with existing cybersecurity models**

At most companies, chief information officers, chief information-security officers (CISOs), and their teams have sought to establish cybersecurity as an enterprise-grade service. What does that mean? They have consolidated cybersecurity-related activities into one or a few organizations. They have tried to identify risks and compare them with enterprise-wide risk appetites to understand gaps and make better decisions about closing them. They have created enterprise-wide policies and supported them with standards. They have established governance as a counterweight to the tendency of development teams to prioritize time to market and cost over risk and security. They have built security service offerings that require development teams to create a ticket requesting service from a central group before they can get a vulnerability scan or a penetration test.

All these actions have proven absolutely necessary to the security of an organization. Without them, cybersecurity breaches occur more frequently—and often, with more severe consequences. The needed

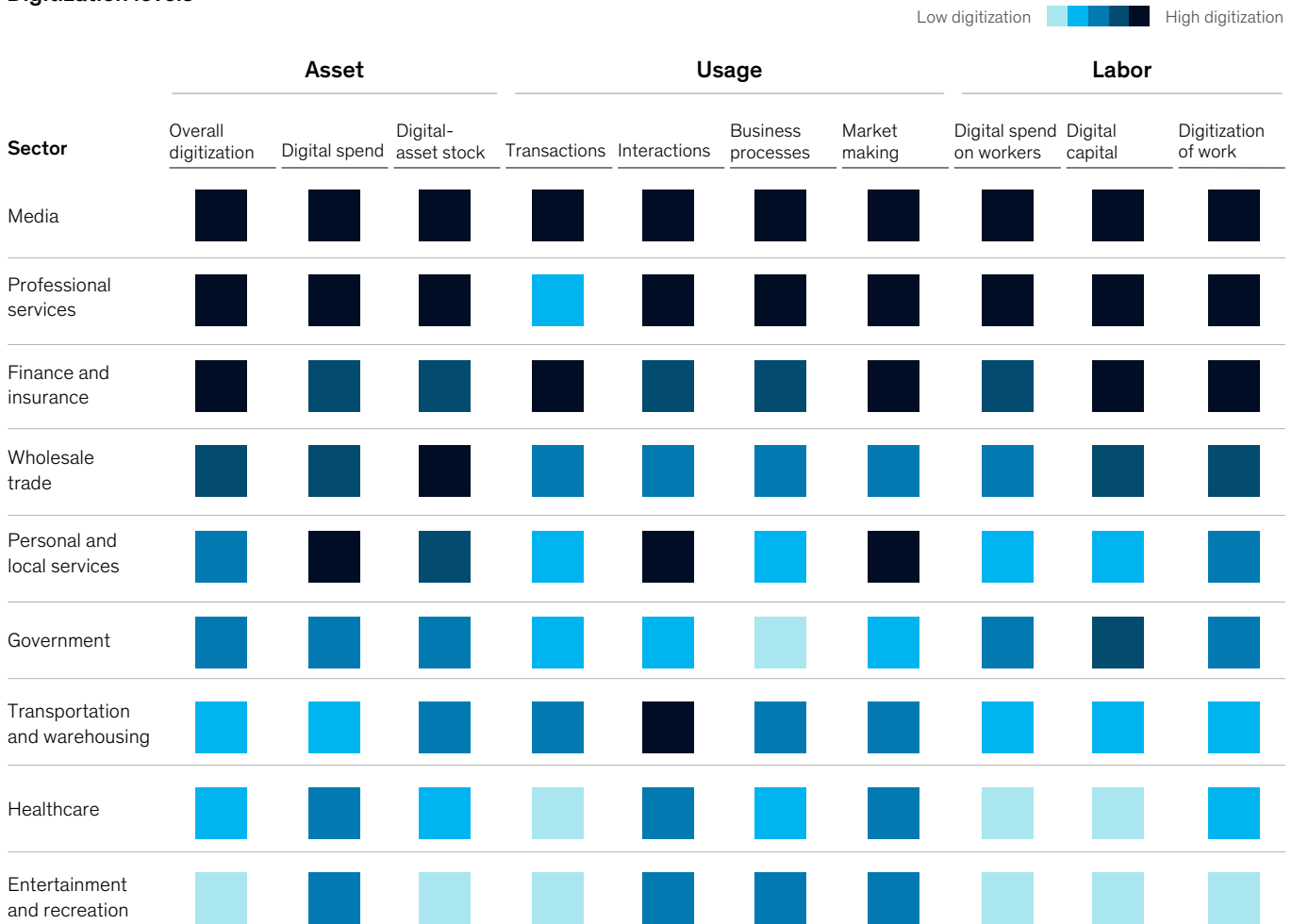
---

<sup>1</sup> An application programming interface is software that allows applications to communicate with each other, sharing information for a purpose.

Exhibit 1

**Across sectors, companies are digitizing, with profound implications for cybersecurity functions.**

**Digitization levels**



Source: Appbrain; Blue Wolf; ContactBabel; eMarketer; Gartner; IDC; LiveChat; US Bureau of Economic Analysis; US Bureau of Labor Statistics; US Census Bureau; Global Payments Map by McKinsey; McKinsey Social Technology Survey; McKinsey analysis; McKinsey Global Institute analysis

actions, however, exist in tension with the emerging digital-enterprise model—the outcome of an end-to-end digital transformation—from the customer interface through the back-office processes. As companies seek to use public-cloud services, they often find that security is the “long pole in the tent”—the most intractable part of the problem of standing applications on public-cloud infrastructure.

At one financial institution, development teams were frustrated with the long period needed by the security team to validate and approve incremental items in their cloud service provider’s catalog for production usage. Developers at other companies have puzzled over the fact that they can spin up a server in minutes but must wait weeks for the vulnerability scan required to promote

their application to production. IT organizations everywhere are finding that existing security models do not run at “cloud speed” and do not provide enough specialized support to developers on issues like analytics, RPA, and APIs (Exhibit 2).

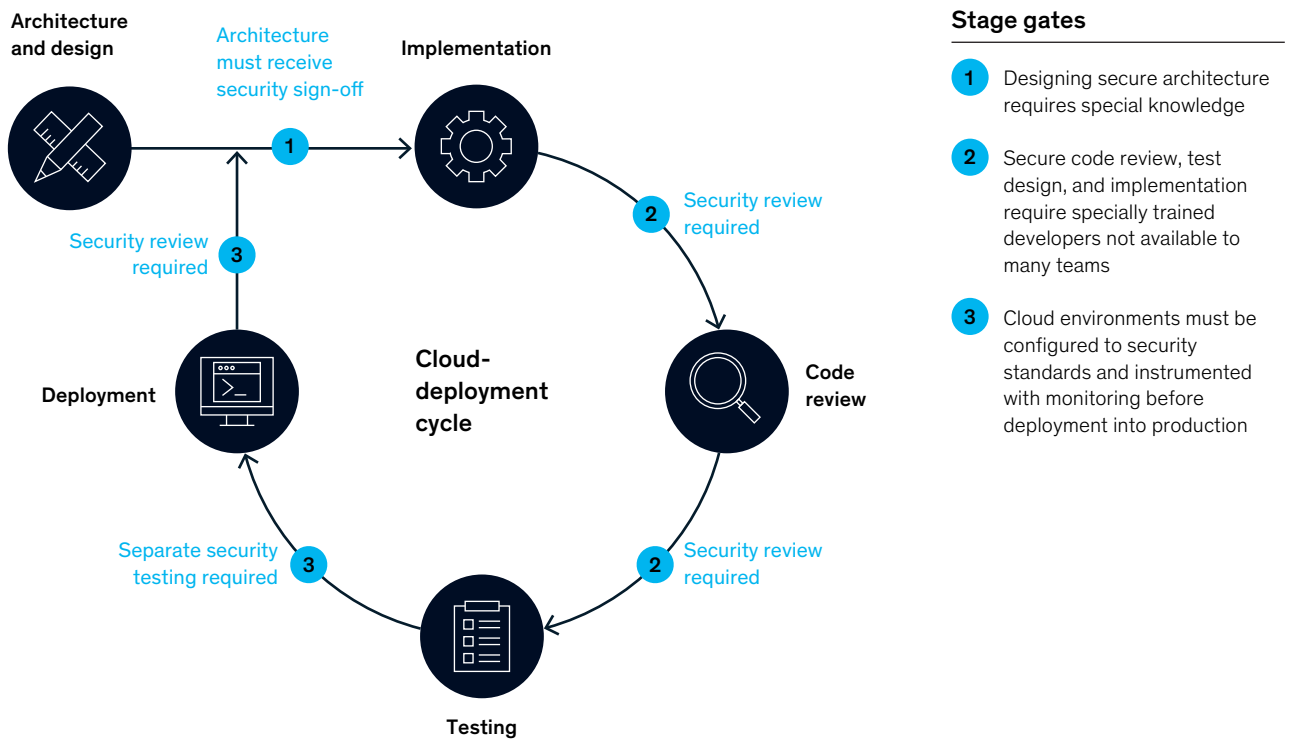
The misalignment between development and cybersecurity teams leads to missed business opportunities, as new capabilities are delayed in reaching the market. In some cases, the pressure to close the gap has caused increased vulnerability, as development teams bend rules to work around security policies and standards.

## Cybersecurity for the digital enterprise

In response to aggressive digitization, some of the world’s most sophisticated cybersecurity functions are starting to transform their capabilities along the three dimensions we described: using quantitative risk analytics for decision making, building cybersecurity into the business value chain, and enabling the new technology operating platforms that combine many innovations. These innovations include agile approaches, robotics, cloud, and DevOps (the combination of software development and IT operations to shorten development times and deliver new features, fixes, and updates aligned with the business).

Exhibit 2

### Current cybersecurity operating models do not operate at ‘cloud speed.’



#### Activities

Architecture and design	Implementation	Code review	Testing	Deployment
<ul style="list-style-type: none"> <li>Analyze resource availability from cloud service provider</li> <li>Analyze capacity requirements</li> <li>Develop initial solution design</li> <li>Design interfaces</li> </ul>	<ul style="list-style-type: none"> <li>Instantiate development and testing environments</li> <li>Begin solution implementation</li> </ul>	<ul style="list-style-type: none"> <li>Review code</li> <li>Conduct automated code scanning</li> <li>Accept code into code base</li> </ul>	<ul style="list-style-type: none"> <li>Develop test cases</li> <li>Do continuous testing</li> <li>Fix bugs and errors; make changes</li> <li>Do regression testing</li> </ul>	<ul style="list-style-type: none"> <li>Instantiate cloud infrastructure</li> <li>Establish cloud services</li> <li>Deploy production application</li> <li>Do final testing</li> </ul>

### Using quantitative risk analytics for decision making

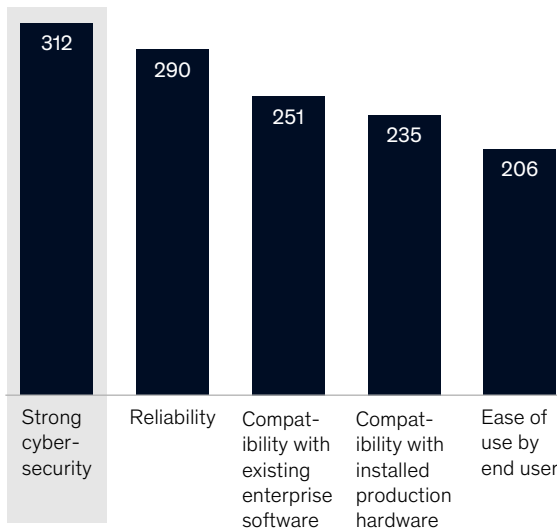
At the core of cybersecurity are decisions about which information risks to accept and how to mitigate them. Traditionally, CISOs and their business partners have made cyberrisk-management decisions using a combination of experience, intuition, judgment, and qualitative analysis. In today's digital enterprises, however, the number of assets and processes to protect, and the decreasing practicality and efficacy of one-size-fits-all protections, have dramatically reduced the applicability of traditional decision-making processes and heuristics.

In response, companies are starting to strengthen their business and technology environments with quantitative risk analytics so they can make better, fact-based decisions. This has many aspects. It

Exhibit 3

### Priority requirements have changed for acquiring Internet of Things products: Cybersecurity has moved to the top.

Top 5 priorities when buying IoT products,<sup>1</sup> number of survey responses



<sup>1</sup> IoT = Internet of Things. Besides basic functionality.

Source: McKinsey 2019 IoT Pulse Survey of more than 1,400 IoT practitioners (from middle managers to C-suite) who are executing IoT at scale (beyond pilots). Composition was 61% from US, 20% from China, and 19% from Germany, with organizations of \$50 million to more than \$10 billion in revenue. This question on IoT-product purchases received 1,161 responses.

includes sophisticated employee and contractor segmentation as well as behavioral analysis to identify signs of possible insider threats, such as suspicious patterns of email activity. It also includes risk-based authentication that considers metadata—such as user location and recent access activity—to determine whether to grant access to critical systems. Ultimately, companies will start to use management dashboards that tie together business assets, threat intelligence, vulnerabilities, and potential mitigation to help senior executives make the best cybersecurity investments. They will be able to focus those investments on areas of the business that will yield the most protection with the least disruption and cost.

### Building cybersecurity into the business value chain

No institution is an island when it comes to cybersecurity. Every company of any complexity exchanges sensitive data and interconnects networks with customers, suppliers, and other business partners. As a result, cybersecurity-related questions of trust and the burden of mitigating protections have become central to value chains in many sectors. For example, CISOs for pharmacy benefit managers and health insurers are having to spend significant time figuring out how to protect their customers' data and then explaining it to those customers. Likewise, cybersecurity is absolutely critical to how companies make decisions about procuring group health or business insurance, prime brokerage, and many other services. It is the single most important factor companies consider when purchasing Internet of Things products (Exhibit 3).

Leading companies are starting to build cybersecurity into their customer relationships, production processes, and supplier interactions. Some of their tactics include the following:

- Use design thinking to build secure and convenient online customer experiences. For example, one bank allowed customers to customize their security controls, choosing simpler passwords if they agreed to two-factor authorization.

- Educate customers about how to interact in a safe and secure way. One bank has a senior executive whose job it is to travel the world and teach high-net-worth customers and family offices how to prevent their accounts from being compromised.
  - Analyze security surveys to understand what enterprise customers expect and create knowledge bases so that sales teams can respond to customer security inquiries during negotiations with minimum friction. For instance, one software-as-a-service provider found that its customers insisted on having particularly strong data-loss-prevention (DLP) provisions.
  - Treat cybersecurity as a core feature of product design. For instance, a hospital network would have to integrate a new operating-room device into its broader security environment. Exhibit 4 presents an example of how security is embedded in a product-development process.
  - Take a seamless view across traditional information security and operational technology security to eliminate vulnerabilities. One auto-parts supplier found that the system holding the master version of some of its firmware could serve as an attack vector to the fuel-injection systems it manufactured. With that knowledge, it was able to put additional protections in place. Pharma companies have found that an end-to-end view of information protection across their supply chains was needed to address certain key vulnerabilities (Exhibit 5).
  - Use threat intelligence to interrogate supplier technology networks externally and assess risk of compromise.
- Done in concert, these actions yield benefits. They enhance customer trust, accelerating their adoption of digital channels. They reduce the risk of customers or employees trying to circumvent security controls. They reduce friction and delays

Exhibit 4

## How to embed security into a product-development process.

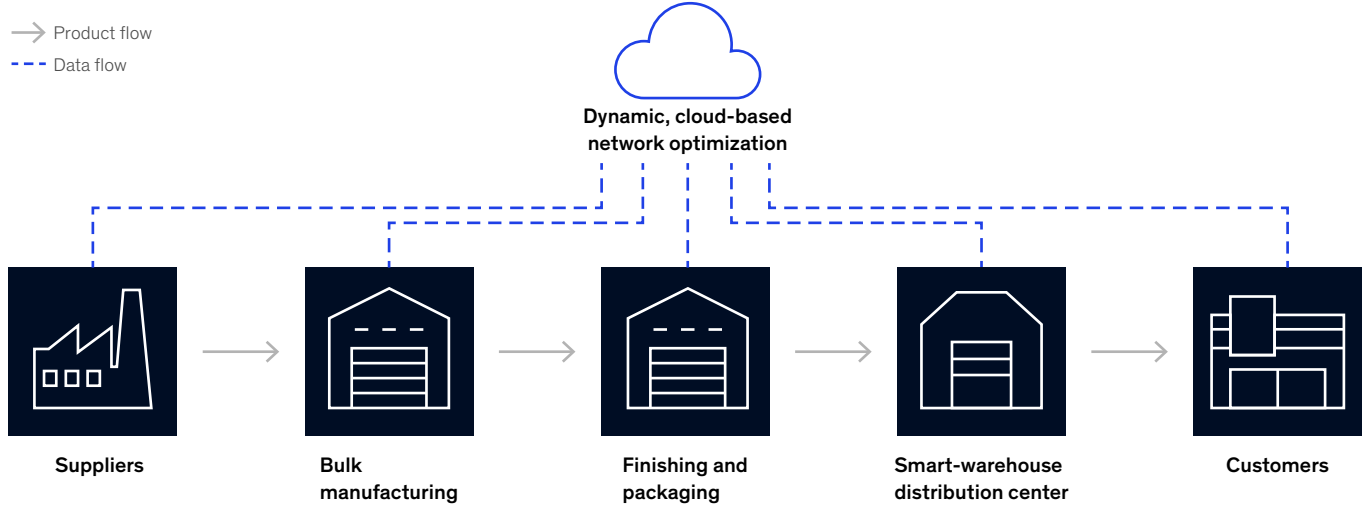
### From treating security and privacy as afterthoughts ...

### ... to incorporating them by designing and building an agile security-and-privacy model

Developers are unclear when security and privacy requirements are mandatory	Product owners don't consider security and privacy tasks during sprint planning	<b>Requirements</b>	Prioritize security and privacy tasks according to product risk level	Make product owners aware of need to prioritize security and privacy tasks and be accountable for their inclusion in releases
		<b>Design</b>		
Unclear how to handle distribution of tasks within development team	Chief information-security and privacy officers (CISPOs) have limited capacity to support development teams	<b>Development</b>	Security and privacy champions (tech leads) assist teams in distributing tasks	Add capacity through CISPOs, who clarify security and privacy requirements with champions and product owners
No unified, real-time, standardized monitoring of state of security and privacy tasks		<b>Testing</b>	Product-assessment dashboards give developers real-time views of security and privacy within products	
Security and privacy needs are often dealt with before deployment, causing launch delays	Teams unclear how often to engage CISPOs	<b>Deployment</b>	Launch delays eliminated as security and privacy tasks are executed across life cycles	Simplified predeployment activities with CISPOs only for releases meeting risk criteria
Unclear accountability for security and privacy in product teams	Lack of integration in security and privacy tool sets introduces complexity	<b>Throughout process</b>	Define and communicate roles and responsibilities during agile ceremonies	Integrate and automate security- and privacy-related testing and tracking tools

**An end-to-end view of information across the pharma supply chain is needed to address vulnerabilities.**

**Supply chain**



● Advanced business capability      ● Resulting cyberrisks

**Suppliers**

- Predictive supplier risk protection
- Risk of exposed vendor details and trade secrets

**Bulk manufacturing**

- Yield optimization through advanced analytics and digitized operations
- Hacking of legacy equipment
- Unauthorized changes in safety or compliance regulations
- Loss of intellectual property and competitive advantage

**Finishing and packaging**

- Fully integrated and automated production
- Attack on process, leading to shutdowns or errors
- Transition from closed to open systems prompts new security risks

**Customers**

- No-touch order management
- Leak of customer data, leading to loss of customer trust and competitive data

**Overarching technologies**

- Machine-learning forecasting and integrated production planning
- Inaccurate business decisions and bad-actor access
- Real-time monitoring
- Unauthorized monitoring of processes and leakage of business decisions

as suppliers and customers negotiate liability and responsibility for information risks. They build security intrinsically into customer-facing and operational processes, reducing the “deadweight loss” associated with security protections.

**Enabling an agile, cloud-based operating platform enhanced by DevOps**

Many companies seem to be trying to change everything about IT operations. They are replacing traditional software-development processes with agile methodologies. They are repatriating

engineering talent from vendors and giving developers self-service access to infrastructure. Some are getting rid of their data centers altogether as they leverage cloud services. All of this is being done to make technology fast and scalable enough to support an enterprise’s digital aspirations. In turn, putting a modern technology model in place requires a far more flexible, responsive, and agile cybersecurity operating model. Key tenets of this model include the following:

- Move from ticket-based interfaces to APIs for security services. This requires automating every possible interaction and integrating

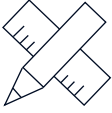




cybersecurity into the software-development tool chain. That will allow development teams to perform vulnerability scans, adjust DLP rules, set up application security, and connect to identify and gain access to management services via APIs (Exhibit 6).

- Organize security teams into agile scrum or scrumban teams that manage developer-recognizable services, such as identity and access management or DLP. Also, recruiting development-team leaders to serve as product owners for security services, just as business managers are product owners for customer journeys and customer-oriented services, can help.
- Tightly integrate security into enterprise end-user services, so that employees and contractors can easily obtain productivity and collaboration tools via an intuitive, Amazon-like portal.
- Build a cloud-native security model that ensures developers can access cloud services instantly and seamlessly within certain guardrails.
- Collaborate with infrastructure and architecture teams to build required security services into standardized solutions for massive analytics and RPA.
- Shift the talent model to incorporate those with “e-shaped” skills—cybersecurity professionals with several areas of deep knowledge, such as

Exhibit 6

## Automation, orchestration technology, and application programming interfaces can eliminate manual security processes and interactions.

### Automation opportunities in a notionally secure DevOps model

	 <b>Architecture and design</b>	 <b>Implementation</b>	 <b>Code review</b>	 <b>Testing</b>	 <b>Deployment</b>
<b>App application programming interfaces (APIs)</b>	API-configurable application-level controls designed into new applications	APIs for configuration and debugging (eg, test instrumentation) added during implementation phase	Automated code-review systems modified to search for application-specific threat scenarios	Automated and configurable security test cases added to nightly testing regime	Fully configured, production-ready application possible via API calls alone
<b>Process APIs</b>	New application-level API options added to deployment-configuration process	Configurable security tests added to nightly testing regime	Configurable automated code reviews added to precommit/preacceptance process for newly written code	Nightly testing results collected and curated for individual developers/teams via configurable test-management system	Predeployment security-review process replaced by automated tests and configuration checks
<b>Infrastructure APIs</b>	API for deployment and instantiation processes rearchitected to accommodate new applications	Configuration options for instantiation of automated, project-specific development environment made available	Automated code scanning implemented for deployed web applications to maintain quality and code integrity	Cloud environments regularly tested for security via automated vulnerability assessment and identification tools	Security tools and configuration options applied via API to new environments at deployment time

Security-trained developers and engineers enable automation and orchestration throughout cloud-development, -deployment, and -operations phases

## How a large biopharma company built cybersecurity capabilities to enable a digital enterprise

A large biopharma company had recently concluded a major investment program to enhance its foundational cybersecurity capabilities, dramatically reducing its risk profile. However, the business strategy began to evolve in new ways, with expanding online consumer relationships, digitally enabled products, enhanced supply-chain automation, and massive use of analytics. The company now needed new cybersecurity capabilities that would both address new business risks and facilitate business and technology innovation.

To get started, the cybersecurity team engaged a broad set of business partners, capturing current and planned strategic initiatives. It then mapped out the new risks that these initiatives would create and the ways in which cybersecurity protections

might slow or block the capture of business opportunities. At the same time, the cybersecurity team looked at a broad set of emerging practices and techniques from the pharma industry and other sectors, including online services, banking, and advanced manufacturing. Based on all this, it developed an overarching vision for how cybersecurity could protect and enable the company's digital agenda, and it prioritized 25 initiatives. Some of the most important were the following:

- collaborating with the commercial team to build patient trust by designing security into online patient journeys
- collaborating with the manufacturing team to enhance transparency into configuration of plant assets

- collaborating with the broader technology team to create the application programming interfaces (APIs) and the template to ensure secure configuration of systems running in the public cloud
- dramatically expanding automation of the security environment to reduce time lags and frustrations developers and users experienced when interacting with the cybersecurity team

The cybersecurity team then used its vision and initiatives to articulate to senior management how it could enable the company's digital business strategy and the support and assistance it would require from other organizations to do so.

in integrative problem solving, automation, and development—as well as security technologies.

Taken together, these actions will eliminate roadblocks to building digital-technology operating models and platforms. Perhaps more important, they can ensure that new digital platforms are inherently secure, allowing their adoption to reduce risk for the enterprise as a whole (see sidebar, “How a large biopharma company built cybersecurity capabilities to enable a digital enterprise”).

With digitization, analytics, RPA, agile, DevOps, and cloud, it is clear that enterprise IT is evolving rapidly and in exciting and value-creating ways. This evolution naturally creates tension with existing cybersecurity operating models. For organizations to overcome the tension, they will need to apply quantitative risk analytics for decision making, create secure business value chains, and enable operating platforms that encompass the latest innovations. These actions will require significant adaptation from cybersecurity organizations. Many of these organizations are still in the early stages of this journey. As they continue, they will become more and more capable of protecting companies while supporting the innovative goals of the business and IT teams.

**James M. Kaplan** is a partner in McKinsey's New York office, **Wolf Richter** is a partner in the Berlin office, and **David Ware** is an associate partner in the Washington, DC, office.

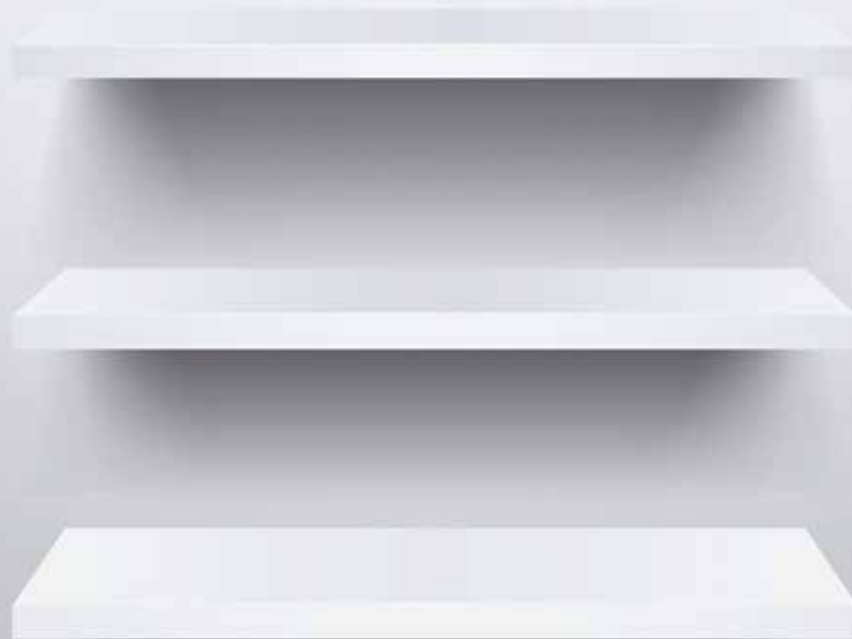
Copyright © 2019 McKinsey & Company. All rights reserved.



# Securing software as a service

Here is how SaaS providers can meet the security needs of their enterprise customers.

*by Rich Cracknell, James M. Kaplan, Wolf Richter, Lucy Shenton, and Celina Stewart*



**Companies are rapidly adopting** software as a service (SaaS) in place of purchasing commercial off-the-shelf (COTS) software. Companies using SaaS rely on SaaS vendors to host their applications in the cloud instead of running them in their own data centers. Industry analysts estimate that the SaaS market will grow by more than 20 percent annually, reaching nearly \$200 billion by 2024, a level that would represent nearly one-third of the overall enterprise-software market. With enterprise values for SaaS businesses reaching approximately seven times forward revenue, software companies are racing to convert from on-premises to SaaS-based delivery models.<sup>1</sup>

Most companies, therefore, will eventually confront the cybersecurity risks inherent in the SaaS approach. These are different risks from those posed by on-premises COTS software. In building COTS software, the vendor takes responsibility for removing security vulnerabilities from the application code. The customer, however, installs the software, configures it, and takes responsibility for running it in a secure infrastructure. For SaaS offerings, the vendor takes on many of the security responsibilities previously assumed by the customer.

Companies do not always feel comfortable with the indirect relationship to cybersecurity risk that SaaS presents, mediated as it is through vendor-based protections. More important, SaaS vendors have not always ensured that their products meet their customers' security requirements. That is the story that emerged from our survey of cybersecurity professionals from companies seeking to adopt SaaS solutions.<sup>2</sup> Their responses also provide insights into how enterprises should think about security in a SaaS world and important clues for SaaS vendors on how to earn the confidence of their enterprise customers.

## **The security challenges of software as a service for adopting companies**

Our survey polled chief information-security officers (CISOs) and other cybersecurity professionals from more than 60 companies of varying size in a range of industries. We wanted to understand how companies experienced SaaS offerings and how they responded to security challenges. Almost universally, respondents confirmed what we had suspected: they have increased their focus on security for SaaS offerings, emphasizing capabilities at the intersection of the vendors' and their own security environments. They expressed a fair amount of frustration with shortcomings in vendors' cybersecurity capabilities, which often caused delays in contracting and implementation. In their view, SaaS vendors need to take a much more customer-centric approach to security, making it easier to understand their products' security capabilities, easier to integrate them with the rest of the enterprise-security environment, and easier to configure them in a secure and compliant way.

All the companies we spoke with had already begun to make the transition to SaaS offerings. About half had used products from 20 or fewer SaaS vendors, and about a quarter from more than 80. Almost all companies surveyed were deploying SaaS offerings in at least one major area, especially office automation, IT-services support, and niche business applications (Exhibit 1).

Many security executives said that their organizations were not ready to use SaaS in some critical domains, however, because of the potential risks. These include enterprise-resource-planning applications, where downtime can prevent the entire business from functioning. Similar concerns were raised for engineering- or manufacturer-related applications. For health-

---

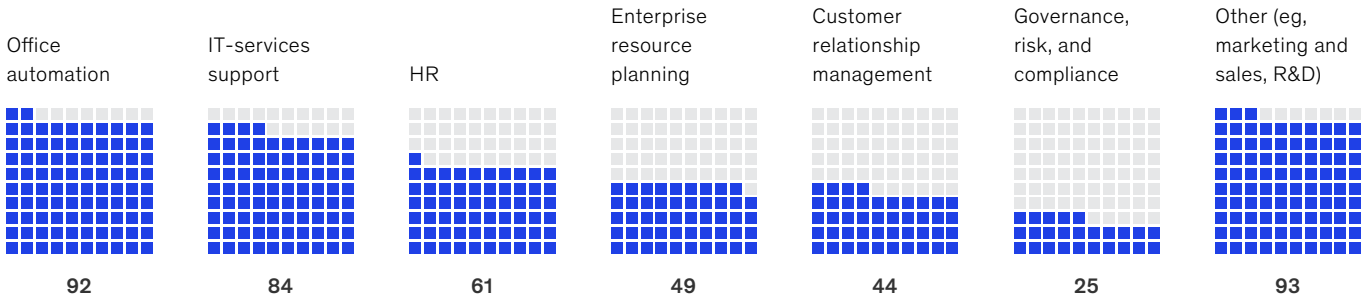
<sup>1</sup> KBV research cited in "Software as a service (SaaS) market to reach a market size of \$185.8 billion by 2024: KBV Research," PR Newswire, December 19, 2018, [prnewswire.com](http://prnewswire.com); *Enterprise software market research report—global forecast 2023*, Market Research Future, May 2019, [marketresearchfuture.com](http://marketresearchfuture.com); "Just where are SaaS companies priced after the 2018 correction?," Tomasz Tunguz, December 26, 2018, [tomtunguz.com](http://tomtunguz.com).

<sup>2</sup> 2019 McKinsey Customer Perspectives on SaaS Survey of chief information-security officers (and managers responsible for cloud security or vendor security) from more than 60 organizations. More than half of the participants were from companies in financial services, insurance, pharma, and health services, with the rest spread across the government, industrial, and tech sectors. Each third (approximately) of the responding companies had respective annual IT budgets of \$500 million and above, \$50 million to \$500 million, and less than \$50 million. Most respondents were from companies based in the United States. Differences in size, geography, and sector apart, however, the companies largely expressed similar concerns.

Exhibit 1

**Surveyed enterprises most commonly used software as a service for office automation, IT-services support, and niche business applications.**

Level of SaaS<sup>1</sup> adoption by usage type, % of respondents (n = 61)



<sup>1</sup> Software as a service.

Source: McKinsey Customer Perspectives on SaaS Survey

related applications and applications that may contain M&A information, the biggest barriers to SaaS adoption concern data confidentiality.

**Priorities in attempting to secure software as a service**

In communications with SaaS vendors, most respondents use questionnaires to gauge security capabilities but criticize the approach as imprecise, incomplete, and overly time consuming. Security executives tend to focus on four key issues when confronting SaaS capabilities: encryption and key management, identity and access management (IAM), security monitoring, and incident response (Exhibit 2). Notable is that each of these issues has more to do with the interface between the customer and the SaaS provider than with the providers' intrinsic technical protections, such as code security and end-point protection.

**Encryption and key management**

Applications running in the cloud and data stored there are not protected by a traditional corporate-security perimeter of firewalls and the like. As a result, security becomes essentially reliant on encryption and management of the keys that provide access to encrypted data. Our interviews

revealed that most companies, especially large ones, do not entrust SaaS providers to host and manage their security keys. The majority prefer to hold their keys on premises through a hardware security module, retain management control of cloud-hosted keys, or use a combination of methods (Exhibit 3). These approaches allow companies to control access to sensitive information. It also ensures that government agencies cannot gain access to and unencrypt their data without contacting them first.

The survey further revealed that companies want a degree of sophistication in key management so that they can grant access to data for a certain period of time or revoke access quickly. This preference again emphasizes that most respondents want to exercise full control over their sensitive information.

**Identity and access management**

Identity management is the act of confirming that each user is the person they purport to be. Access management is the determination that a user does or does not have legitimate rights to retrieve data or use an application. As important as both identity management and access management are on company premises, they are even more important for cloud-based applications.

## Enterprise customers focus on the interface between software-as-a-service providers and their own security environments.

Capabilities that respondents would like to see from SaaS<sup>1</sup> vendors, % of respondents (n = 61)



<sup>1</sup> Software as a service.

Source: McKinsey Customer Perspectives on SaaS Survey and interviews with more than 60 industry leaders

Security executives emphasized that two IAM capabilities are especially important to them. First, they want tight, easily implementable integration between SaaS applications and widely adopted enterprise IAM tools. Companies deploy hundreds or thousands of applications, dozens of which are SaaS applications. They cannot expect users to memorize yet another password for each new SaaS offering that is adopted. They want to allow users to sign into SaaS applications via enterprise-wide IAM platforms, which will provide additional features like two-factor authentication. Second, they need sophisticated, role-based access management,

including the ability to provide selected people with the authority to access certain data or undertake certain transactions within an application.

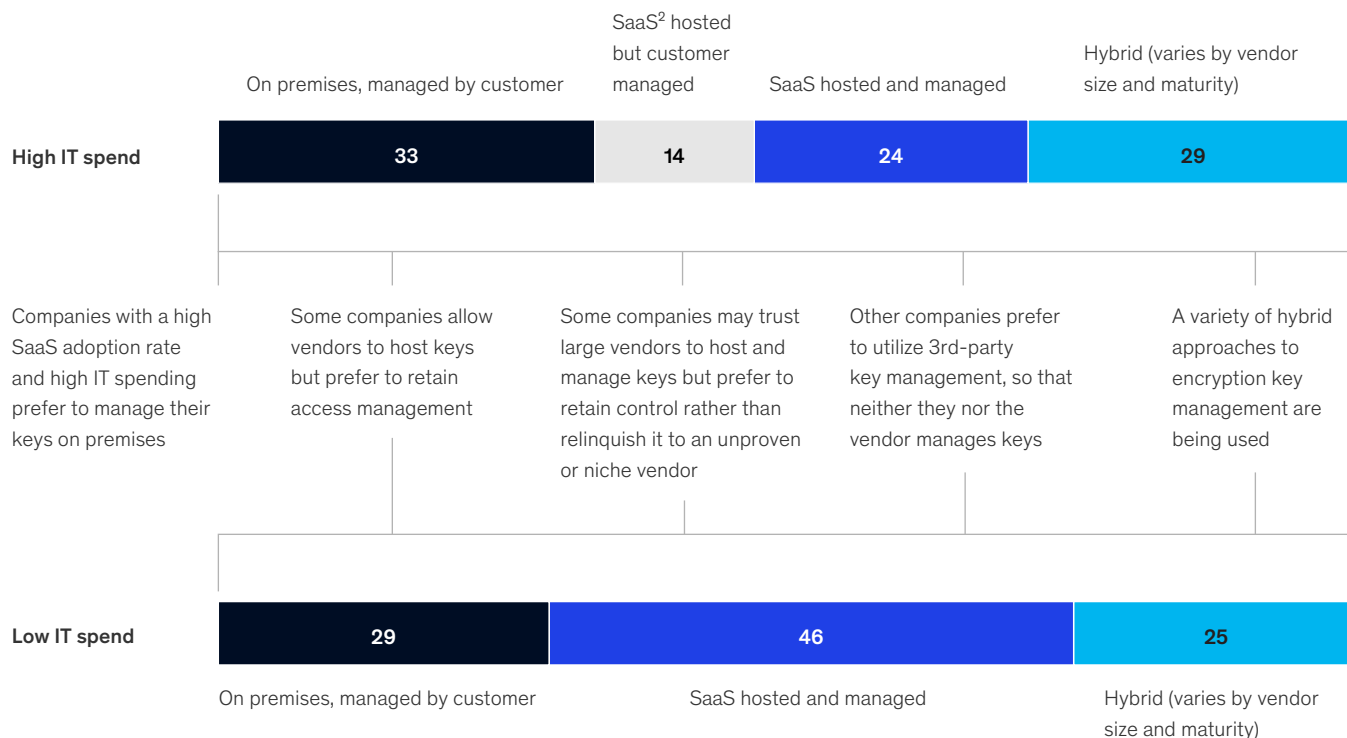
### Security telemetry and monitoring

Increasingly, CISOs acknowledge that they cannot prevent every instance in which security is compromised. They therefore want the necessary transparency to identify and assess emerging security risks quickly and thoroughly. As companies adopt SaaS offerings, data from SaaS providers about usage patterns become critical to this analysis.

Exhibit 3

### Most enterprises do not fully entrust software-as-a-service providers with hosting and managing encryption keys and so use different control methods.

Preferences for hosting and managing encryption keys, by level of estimated IT spending,<sup>1</sup> % of respondents (n = 44)



<sup>1</sup> All IT-spending estimates rely on information from "IT key metrics data 2019: Executive summary," Gartner, December 17, 2018, gartner.com.

<sup>2</sup> Software as a service.

Source: McKinsey Customer Perspectives on SaaS Survey and interviews with more than 60 industry leaders

Security reporting is the baseline capability CISOs demand. They want a clear view—usually consolidated in a dashboard—of the users that have been accessing their data and what they have done with them. Without this kind of transparency, implementing even the best security concepts can be a “nightmare,” as one security executive remarked.

Many security teams seek to integrate data on SaaS usage with external-threat intelligence and information from the rest of their technology environment to determine the actions they must take to protect their company. To accomplish this, the security teams need SaaS providers to offer application programming interfaces (APIs), which will allow them to pull data into their security-operations centers (SOCs) and security-incident-

and-event-management (SIEM) platforms. As a health-services CISO explained, “On-premises security controls are getting extended into the cloud. Only a few SaaS providers allow us to pull logs to go into our SIEM.” A banking CISO said, “I want to integrate with SOC/SIEM. I want something flexible enough to work with hardened SIEM tools, and something capable of integrating as well.” In other words, CISOs want their vendors to make it easier to use APIs for integration. They also want timely service provision as well as accurate security information from their SaaS providers included in service-level agreements.

#### Incident response

Every company can be breached. Therefore, security teams must implement tools and practices

for managing, mitigating, and resolving incidents. Naturally, security monitoring plays a significant role in this, as greater transparency enables better incident response.

Most organizations focus on SOC and SIEM integration. The more sophisticated security organizations we spoke with have dramatically broadened their incident-response requirements to include joint simulations, joint forensic activity, and intelligence sharing. One company even secured the right from one provider to send personnel to the provider's SOC in the event of a major breach.

### **Broader security concerns and pain points**

CISOs also stated broader concerns with SaaS vendors' security capabilities. These include a lack of readiness of many SaaS offerings for integration with the company's larger security environment as well as insufficient transparency on whether SaaS products meet local data-privacy requirements. A further concern surrounds the experience of SaaS sales forces, which CISOs say can be ill informed and sometimes even outwardly deceptive about security-related issues.

#### **Integration is challenging**

Nearly two-thirds of companies express frustration with the process of integrating SaaS products with the rest of their security environments. The trouble spots cited are as follows:

- lack of preexisting connectors to commonly used IAM and SIEM platforms
- insufficient functionality of APIs for obtaining the information required, especially log visibility at the platform level
- poor API documentation, confusing API-usage semantics, and a shortage of relevant code samples
- differently designed APIs for products from the same vendor
- lack of trained vendor personnel to assist in using APIs

CISOs complained of APIs that are not delivered; integration that is not achieved, even when the road map is followed; missing documentation; a lack of active support; and no vendor response when a problem develops. A biotech CISO emphasized "the lack of security monitoring: [SaaS vendors] forget about the confidentiality and integrity aspects of the monitoring."

#### **Limited focus on data privacy**

As major data breaches proliferate and regulatory attention mounts, data privacy is becoming an issue in the decision-making process for SaaS contracting and implementation. Security teams, meanwhile, find vendors scrambling to provide adequate clarity on the data-privacy protections in their offerings. One medical-products CISO pointed out that SaaS providers struggled to fulfill data-residency requirements—identifying the countries where the data are stored. Companies need to know the residency to meet local data regulations.

CISOs often cannot tell whether SaaS products properly meet new data-privacy mandates, including the European Union's General Data Protection Regulation (GDPR), Brazil's General Data Protection Law, and the California Consumer Privacy Act. Companies need to know this information to configure critical features, such as encryption, data purging, and data logging, as they ensure compliance.

Respondents say that the claims SaaS providers make about product compliance are often overstated, so they don't necessarily trust them. A technology company's CISO said, "For things like GDPR, everyone is trying to figure it out; if anyone claims that they are mature in their process around GDPR, I would question this. I would prefer a sense of openness [and] honesty around what SaaS providers are doing and why they believe they are compliant."

#### **Uninformative sales interactions**

Security executives assert that their interactions with SaaS-provider teams on security issues are difficult and frustrating. They say that sales representatives make security claims that don't

appear to be backed up by fact, and that vendors don't have security experts they can talk to. Such experts, who would know the technical specifications of the offerings, are needed to help companies decide how to configure SaaS offerings in a secure way. More than 70 percent of respondents said that uninformed or misleading claims about security capabilities were a cause of dissatisfaction. Reportedly, some sales representatives even misrepresent certifications or customer references. One manufacturing company's CISO said, "I am sick of receiving glossy marketing materials, which are essentially snake oil when it comes to security features . . . many, many vendors will claim their security features are better than [what] a very simple assessment will reveal." Another pointed out examples where simply checking a reference proved that the referenced company had not used security features in the way the sales team had described.

### **Implications on software-as-a-service purchasing and contracting**

SaaS vendors' shortcomings in security capabilities are shaping the ways enterprise customers contract for and use SaaS products. Negotiations about security terms and conditions (T&C) can add weeks or months to contracting processes. Survey respondents said the most challenging issues debated included financial liability for breach events, required cyber-insurance policies, and preferred location for legal proceedings.

Security issues often disqualify providers from consideration. For those that are considered, security remains a major concern; a few of our respondents told us that they had reverted to a provider's on-premises solution because they

could not become comfortable with the security provisions of the SaaS offering. When discussing the deployment of SaaS offerings, security executives mentioned the cost and complexity of the compensating controls they had to put in place to manage the accompanying risk. Many decide to invest in specialized third-party tools to manage encryption keys, ensure compliance with corporate policies, analyze vulnerabilities, enhance encryption, or track data usage for SaaS offerings. CISOs also say that they must expend scarce talent and resources in configuring and managing security offerings to meet their standards.

In a few reported cases, large companies called off planned migrations from an on-premises platform to a SaaS offering for security reasons. In one case, the vendor failed to meet commitments to make the APIs mature for IAM and SIEM integration. After the company had devoted significant resources to use the required APIs, it gave up and reverted to the existing version of the application in order to ensure required performance. In another example, new charges for security-related features were significant enough to sour the business case for adoption of a SaaS offering, causing the company to continue using the on-premises version.

### **Actions software-as-a-service providers can take to meet the security requirements of their enterprise customers**

For all the value that SaaS promises, security concerns limit enterprise customers seeking to make the transition from on-premises solutions to SaaS-based ones. Fortunately, providers can take the following steps to remove barriers to SaaS adoption.

## **Security issues often disqualify providers from consideration.**

## 1. Build agile security capabilities

Every company surveyed expected its SaaS providers to have a robust solution in place, including a secure development life cycle and a secure stack for hosting its application in production. However, changes in software-delivery models have disrupted existing security practices and architectures. As established software vendors adopt agile development methods to improve time to market, earlier practices supporting a waterfall development process—sometimes put in place over decades—are becoming increasingly irrelevant. Since software companies provide their applications via their cloud but also host them on infrastructure provided by hyperscale cloud companies, years and decades of experience designing secure on-premise infrastructure stacks also become less relevant. Finally, the security organization can no longer “inspect for security,” since this delays the process.

SaaS providers must take a number of steps to build agile security capabilities. They must design and build security into their agile development processes. This includes automating security into the development tool chain, placing security champions on scrum teams, and training every developer on secure coding. They must furthermore build an infrastructure operating model with a clear understanding of security ownership, determining what their cloud-infrastructure provider for security will do and what they must do themselves. A secure system configuration in the cloud will be especially critical here. Finally, underpinning all this, SaaS providers must build an agile security organization that enables the business by providing automated security services rather than slowing it down with inspections and rework.

## 2. Adopt a multilevel model for addressing security-related customer inquiries

When asked about the characteristics of best-in-class SaaS vendors on security, 70 percent of cybersecurity professionals cited transparency on security capabilities. They said that in selling, vendors can distinguish themselves by giving informed, straightforward responses regarding security capabilities and after-sale onboarding. They also said that vendors should provide transparency

regarding updates and expected implications for customer systems. Software vendors can meet these expectations with a multilevel model for addressing security-related customer inquiries.

**Level 1.** Partner with third-party security-assessment vendors to make data about security capabilities easily available at a low cost. Some third-party platforms capture more than 1,200 data points about each vendor's security capabilities. SaaS providers have no reason to refrain from sharing this information with potential customers.

**Level 2.** Train the sales force in the basic security features of the offerings and ensure that they respond to security inquiries accurately and intelligently. In addition, vendors need to provide incentives to salespeople that encourage them to ask for expert help rather than provide incorrect or incomplete information.

**Level 3.** Create a specialized team to respond to sales-force inquiries, supported by a robust knowledge base to help answer more complicated questions. Given the importance of API-based integration, this group should act as a developer-support function in many respects. It should also invest in developing code samples and other artifacts that will make it easier for the customer's security teams to implement the vendor's products.

**Level 4.** Provide a clear escalation path to security engineers who can answer the most complicated questions about IAM, telemetry, key management, and other issues.

**Level 5.** Prepare for customer T&C requests. Customers will ask about the assumption of liability, preferred legal venues, and other issues. Vendors need to develop protocols for the circumstances under which they will accept requests, such as which requests will be accepted and from whom. Just as enterprise customers seek to assign prices to security risk, vendors may want to assign costs to special T&C requests. Even if they cannot pass that cost along to the customer, this type of accounting tool can provide an indication of whether a deal is worth making.



### 3. Aggressively facilitate integrations

The day of the stand-alone, monolithic application ended years ago, for security features as well as for the enterprise-technology environment. SaaS vendors should thus make it easier to integrate their offerings with the rest of their customers' security environments. This requires several actions.

*Build a comprehensive set of connectors to relevant security tools.* Major SaaS providers need to have prewired integration capabilities for every major enterprise IAM platform, cloud IAM platform, privileged-access-management platform, and SIEM platform. So equipped, providers will enable customers to implement their products more quickly, less expensively, and with greater confidence that they are not introducing new security vulnerabilities.

*Invest in building better APIs.* Too often, SaaS vendors pay little attention to security APIs. Instead, they should create a consistent security-API model across the products they offer. They should work with customers' security teams to provide the granular capabilities required in the areas of encryption, key management, and telemetry. They should deploy simple, easy-to-understand API semantics backed up by documentation.

*Enhance security-related customer-success teams.* Nearly two-thirds of security executives said that leading vendors were distinguished by the superior technical expertise of their support organizations. This means that vendors should enhance the security skills of the teams that help customers implement their products. In addition to improving customer outcomes, enhanced customer support could lead to more sales.

### 4. Help customers address data privacy

With expanding market and regulatory demands for data privacy, CISOs believe that SaaS vendors have not demonstrated sufficient leadership in

this area. They need these vendors to research thoroughly the regulatory expectations in the markets they participate in and identify the specific actions required to comply. They need vendors to invest in the encryption, key-management, logging, data-tracking, and data-purging capabilities necessary for compliance. They should also guide CISOs on how to implement their products to minimize regulatory risk.

---

Over time, SaaS will largely replace traditional on-premises COTS applications, with enterprises benefiting from faster innovation, reduced complexity, lower operating costs, and massively reduced management spending on obsolete technologies. However, SaaS disrupts the traditional relationship between vendors and customers on security. With the vendor taking on much more security responsibility than before, the security team is put right in the middle of SaaS-adoption decisions. Moreover, companies cannot accept SaaS products as security black boxes. As we have emphasized, they must be able to determine how to integrate them into the rest of their security environments.

Our survey indicates that many SaaS vendors have yet to understand this new reality. They do not communicate well with customers on security, their products are hard to integrate with the rest of the customers' security environments, and they have not taken the lead in helping customers comply with data-privacy expectations. Security issues are causing companies to eliminate certain vendors from consideration, extending procurement processes by weeks and months and adding significant cost and complexity to SaaS deployments. By actively addressing these issues, providers will speed the ongoing migration from traditional on-premises applications to SaaS.

**Rich Cracknell** is a manager of solution delivery in McKinsey's Silicon Valley office; **James M. Kaplan** is a partner in the New York office, where **Celina Stewart** is a cyber solutions senior analyst; and **Wolf Richter** is a partner in the Berlin office, where **Lucy Shenton** is a cyber solutions specialist.

Copyright © 2019 McKinsey & Company. All rights reserved.

# The customer mandate to digitize collections strategies

Customers told us that more calling won't improve lenders' contact and recovery rates. Here's what they said does work.

*by Matt Higginson, Frédéric Jacques, and Glen Kushta*



© John Lamb/Getty Images

**Research into the customer experience** of credit delinquency has helped clarify the path lenders need to take to achieve more effective collections. Essentially, customers told us that their contact preferences and responses are guided by personal considerations that bear little relationship to the risk categories and contact protocols worked out by lenders. Most customers prefer to be contacted and act through digital channels, while a smaller segment remains more responsive to traditional contact methods. From these findings, we have concluded that issuers need to better understand their customers' diverse preferences and then design a sensitive, multichannel contact strategy to address them. The strategy requires coordinated capabilities—in technology and infrastructure; in advanced analytics, machine learning, and automation; and in a well-orchestrated deployment. The object is to deliver tailored messages through the right channels in the right sequence to the right customers. The cost of implementing a true multichannel strategy will amount to a small fraction of the return to issuers—more efficient and effective recoveries and happier customers.

### **A no-regrets response to downward pressures**

As economists and business analysts debate the time of arrival of the next economic downturn, lenders are weighing the implications of a possible contraction. Losses across several important asset classes have already begun to rise, for several reasons. In addition to economic factors, the trend has been fueled by lenders' actions, changing customer preferences, and stronger consumer regulation. During the global economy's long boom period, lenders experienced low losses and consequently tended to underinvest in collections. At the same time, customer contact preferences shifted decidedly to digital channels and away from the traditional methods lenders use for addressing delinquency. Meanwhile, regulators have placed limits on the scope and intensity of collections activities.

While the economic cycle and the regulatory environment are beyond lenders' control, they can

reduce losses stemming from the poor success rate of customer contact. Our experience strongly suggests that lenders need to shift their own methods to match customer preferences—which are clearly for digital channels. In addition to improving outcomes, such a direction change in customer contact would also avoid regulatory repercussions. In the United States, for example, the Consumer Financial Protection Bureau is now proposing a limit of seven calls per customer per week—only a recommendation at this point, but one that would have profound implications for the collections and recovery industry.

Switching to digital-first contact will involve a significant change in collections strategy and operations, taking 12 to 18 months, so we are recommending that institutions get started as soon as possible. Particularly important is improving operational effectiveness of existing resources. Doing so will keep lenders ahead of any approaching down cycle in the macroeconomy. When that does arrive, losses will rapidly accelerate.

### **What the research revealed**

In late 2018, we conducted a survey in North America of customers who were recently delinquent on a credit card in order to understand their experience of collections. The respondents were broadly representative of delinquent card customers in the market and roughly proportional to the relative sizes of the delinquent card population of 12 major issuers. We asked them about their lenders' contact approaches during delinquency, how they responded by channel, their preferred channels for engagement, and the outcomes of each contact attempt in various stages of delinquency.

Our goal was to uncover and explore the effects of mismatches between the contact strategies used by issuers and those preferred by their customers. Our ingoing hypothesis was that the customers' preferred channels were the most effective in debt repayment. The data we received strongly confirmed this.

**Customer experience reveals misalignment of contact strategies**

The responses of 1,000 delinquent customers enabled us to construct representative profiles of the delinquent population for each issuer, including customer risk profiles, days delinquent, and contact strategies used. Clear differences emerged in contact strategies from issuer to issuer in terms of the range of channels employed, the intensity of channel usage, and the sequencing of contact attempts according to risk profiles.

We discovered that most issuers still use traditional contact strategies based on customer balance, risk profile, and days delinquent. Some are beginning to integrate contact preferences and behavioral segmentation into their models. Yet lenders using digital channels such as email and text in early

delinquency largely abandon them after 30 days, switching to traditional channels such as phone calls and letters.

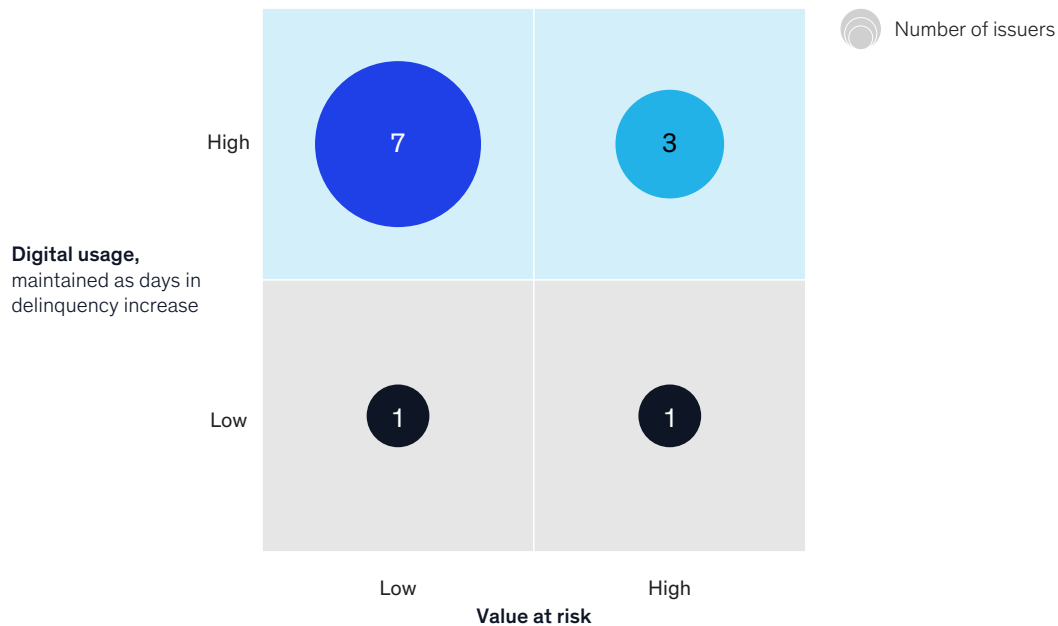
Using survey and issuer data, we plotted the collections landscape. The 12 issuers fell into four quadrants according to two main criteria: the value at risk in each portfolio and the usage of digital channels for contacting delinquent customers. Digital usage was measured according to issuer persistence in contacting customers through the stages of delinquency (Exhibit 1). This was because customers revealed that most issuers use digital channels in the beginning of delinquency but are more likely to revert to traditional channels later on.

The key takeaway from the early part of our research was that customer preferences for digital channels

Exhibit 1

**Issuer and customer data revealed collections profiles for 12 credit-card issuers in terms of value at risk and contact strategies.**

**Issuers by digital usage and value at risk<sup>1</sup>**



<sup>1</sup> Disguised survey results. Digital channels include email, text, mobile-app pop-up, online-banking pop-up, and phone push notification; digital share of contacts for last channel excludes respondents who were less than 30 days in delinquency. Value at risk for each customer is calculated as balance times probability of default (mapped from FICO score). Digital usage measured as sum of digital share of contacts for first and last contact.

Source: S&P Capital IQ; McKinsey analysis

remained pronounced through delinquency and were not aligned to or affected by issuer-assigned risk profiles.

From the customer viewpoint, therefore, issuers lag behind their own digital inclinations. For example, while higher-balance customers are more likely to engage on digital channels such as mobile and online banking, most issuers are contacting only low-risk customers in this way. A handful of issuers—market leaders all—have begun implementing true multichannel contact strategies across the full customer journey. The other issuers still have to capture this opportunity.

**Customers express their engagement preferences**

Although issuers remain wedded to traditional channels, using them even more heavily in later delinquency, their customers expressed a general preference for digital contact—primarily by email, followed by text message—irrespective of the prevailing stage of delinquency. The digital preference is most pronounced among customers with a low delinquent balance.

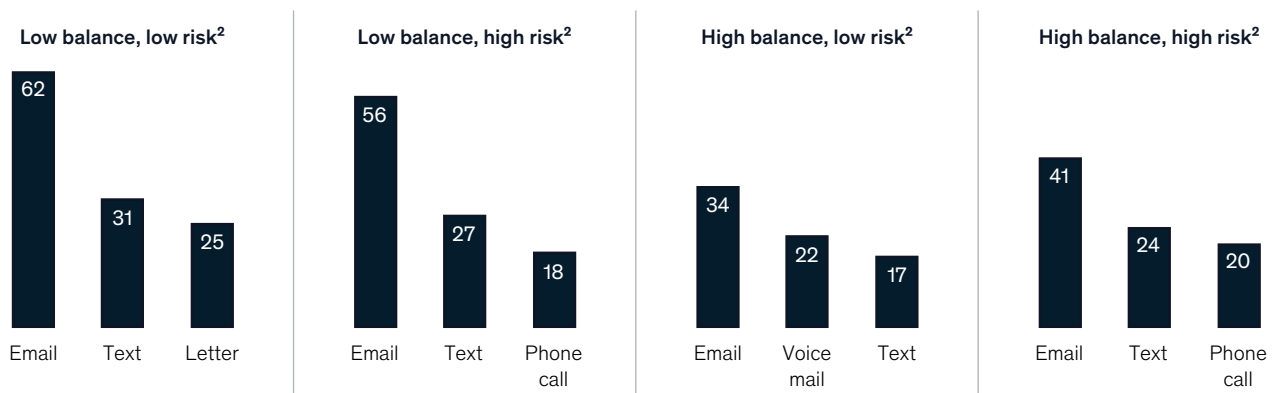
One responding segment did express a preference for traditional contact, however, though not for phone calls. Lower-risk customers—those with better credit scores—preferred impersonal messages in traditional channels, such as letters and voice mails, on which they are able to take action in their own time. Looking more closely at these traditional, or “analog,” customers, we found that they are commonly older (44 years and above), have never used their account digitally or through an app, and ordinarily pay their balance in full. On the other hand, our survey’s “digital” respondents were more commonly between the ages of 25 and 44, have recently used their account online or through an app, and more commonly revolve their balance, usually of \$5,000 or less.

Exhibit 2 shows that credit-card customers most prefer email as a contact channel; this preference is most pronounced among customers with lower balances (less than \$1,000). Unlike the high-risk groups, low-risk respondents prefer to engage through email and text rather than talking with a bank representative on the phone. For banks, the pattern of preferences clearly creates the

Exhibit 2

**Credit-card customers mostly prefer to be contacted by email and text.**

Preferred channels of contact, % of respondents<sup>1</sup>



<sup>1</sup> N = 434 survey respondents. Analysis excludes respondents under 30 days delinquent.  
<sup>2</sup> Balance criteria: low, ≤\$1,000; high, >\$1,000. Risk criteria: low, FICO > 620; high, FICO < 620.

potential for identifying a segment of customers for a self-service channel.

### Matching channels and preferences

Customers in delinquency are sensitive to the contact method chosen by their bank. A deeper, nuanced segmentation of at-risk customers is needed.<sup>1</sup> In our survey, the majority of customers in the sample, whatever their financial position, expressed the preference for engaging with issuers through digital channels. When contacted digitally, they are more likely to make a payment or to pay in full, and this likelihood increases for customers with accounts that are more than 30 days past due (DPD). Most indicated that they are less motivated to take action when contacted through traditional channels, though a minority still prefer to be contacted in this way (by phone call or letter). This distinct traditional population usually pays in full.

Despite customer inclinations, banks are not using the channels that lead to the best collections outcomes.<sup>2</sup> The survey revealed that the majority of issuer-initiated contacts with delinquent customers are made through traditional channels (65 percent),

including these categories: 32 percent by phone call, 16 percent by letter, and 15 percent by voice mail. Digital channels are used less often (35 percent), led by email (17 percent), and trailed by text (7 percent) and mobile push (6 percent). However, these channels resulted in much higher response rates, with customers taking action (making a payment) 73 percent of the time (Exhibit 3).

### High success rates from neglected channels

The action rates—a partial or full payment—achieved by traditional channels were reported as 48 percent for phone call, 50 percent each for voice mail and letter, and a whopping 91 percent for the ATM pop-up, the least-used traditional channel. Digital channels, on the other hand, have a much higher success rate overall: while only 58 percent of respondents made a partial or full payment when contacted by email, the success rates for both online banking and mobile-app pop-up were each 92 percent; they were 88 percent for mobile push and 77 percent for text.

Issuer contact through digital channels more often achieved full as opposed to partial payment. Here the success rate for traditional channels was around 12 percent overall for phone call, voice mail,

<sup>1</sup> Ignacio Crespo and Arvind Govindarajan, "The analytics-enabled collections model," *McKinsey on Risk*, April 2018, McKinsey.com.

<sup>2</sup> Matt Higginson, Frédéric Jacques, Marta Matecsa, and Davide Tesini, "Going digital in collections to improve resilience against credit losses," *McKinsey on Risk*, April 2019, McKinsey.com.

#### Exhibit 3

**The overall customer preferences for contact through email, text messaging, online banking, and mobile retain strength in late delinquency.**

65%

of issuer-initiated contact in late delinquency (30+ days past due) is made through traditional channels—despite lower response rates

73%

of customers in late delinquency took action (made a payment) when contacted through digital channels

Source: McKinsey Survey of Credit-Card Customers at North American Financial Institutions, 2018

and letter. The rates for full payment from digital channels varied but were uniformly higher: 19 percent for email, 46 percent for online banking, 44 percent for mobile push, 20 percent for mobile app, and 19 percent for text.

**Sensitivity by segment**

The survey respondents revealed that issuer sensitivity to the preferences of the two (survey-driven) customer segments—digital and traditional—substantially improves payment outcomes (Exhibit 4). For example, digital customers were 12 percent more likely to make a payment when contacted through their preferred channels; they also paid in full more often when contacted in this way. With traditional customers, issuers had 17 percent better results with phone and letter contact.

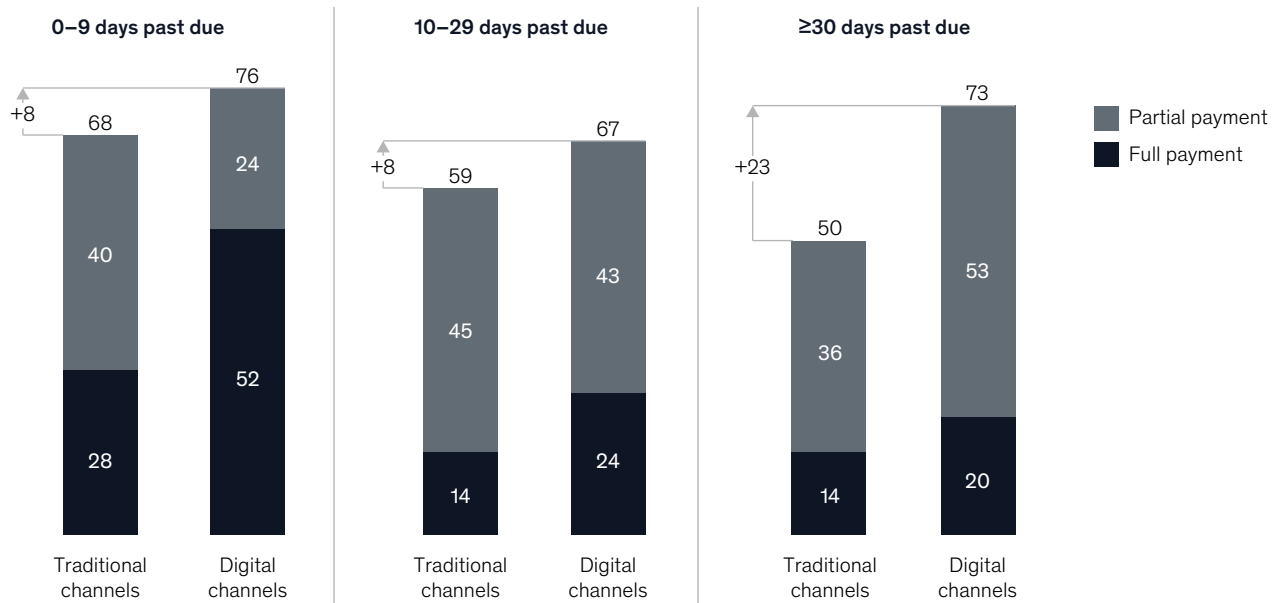
In terms of DPD, the effectiveness of contacting digital-first customers through their preferred channels improves most significantly in the 30-plus DPD category (by 23 percent). Contact effectiveness declines almost as dramatically in this category when digital customers are contacted through traditional channels (–18 percent). While the overall payment rate remains similar for these customers, digital contacts result in more partial payments as customers become more delinquent.

Issuers assume traditional channels will be more effective at this point, but our survey indicates that the approach is not optimal for resolving customer delinquency. The survey suggests that the digital-to-traditional channel shift after early delinquency will likely yield 12 percent fewer payments from the great majority of customers

Exhibit 4

**Contacting customers through preferred digital channels improves effectiveness most significantly in the segment of accounts that were 30-plus days past due.**

Payments made on last contact, %



(90 percent) who prefer digital contact. This supermajority are also more likely to make only partial payments when contacted traditionally.

The differences noted in our survey were the result of only crude segmentation of customers according to simple markers of contact preference. Without exception, issuers hold many more pieces of data about their customers than could be harvested in our survey, suggesting even greater improvement in collections effectiveness by following this proposed approach.

### **An effective multichannel contact strategy**

To capture the collections opportunities indicated in customer responses to our survey, issuers need an effective multichannel contact strategy. Such a strategy does not take a one-size-fits-all approach to contacting delinquent customers, but it does recognize the superior effectiveness of and preference for digital channels overall. Most issuers, however, are still reliant on an approach centered around traditional contact methods.

The strategy depends on three kinds of capabilities and actions. First, the *technology and infrastructure* must be in place to support the development of the needed digital channels and self-service functionality. Second, capabilities in *data analytics*, *artificial intelligence (AI)*, and *automation* enable

the identification and segmentation of customer types and preferences. Finally, the *contact strategy* must be deployed, addressing the segments appropriately, through the correct channels, with the right messages, in the proper sequence by segment.

The action steps needed in the three areas are as follows:

#### 1. *Technology and infrastructure:*

- **Build digital channels.** Issuers need to expand digital assets to enable more email, text, mobile app, and online banking. Efforts to maximize customer-qualification rates for digital-contact channels—including opt-in or -out, skip, and app access—are also highly recommended.
- **Invest in self-service capabilities.** Online banking and virtual collections agents could increase payments and reduce costs for call centers while improving customer satisfaction. Most customers prefer to engage through an impersonal channel: if alerted by email and text, they can then take action by themselves.

#### 2. *Data analytics, AI, and automation:*

- **Create profiles and contact sequencing.** Data analytics and AI can help banks build customer profiles, including preferences, balance history, and DPD. Based on these

**To capture the collections opportunities indicated in customer responses to our survey, issuers need an effective multichannel contact strategy.**



attributes, extended digital approaches (including sequence of contact, such as text, then email), aided by automated processes, can be crafted.

- **Maintain sensitivity by profile.** A smaller group with traditional contact preferences will be less inclined to pay when contacted digitally; these should be prioritized early in delinquency with consistent phone and letter contacts. They might also pay in full voluntarily.
- **Apply machine learning.** Machine-learning algorithms for customer preferences can aid in shaping the most appropriate communications.

### 3. *Designing and deploying the multichannel strategy:*

- **Design a truly integrated multichannel contact strategy.** This is done through improved sequencing and coordination across channels. A methodical approach should be applied to support the selection and matching of the right customer with the right channel, the right time, and the right offer. Future iterations should accommodate subsequent test-and-response insights, preferably in near real time.

- **Tailor messaging.** The content, tone, and style of digital communications should be carefully crafted, in recognition that digital-first customers might be avoiding embarrassment or confrontation and need nuanced outreach (such as a softer tone).

---

Through our research, customers conveyed a clear message to issuers: to protect against credit losses, contact strategies should be shifted to match customer preferences. The path to a better customer outcome mainly involves expanding the use of digital channels for most customers while preserving traditional channels to address a smaller but important segment. As market leaders already understand, an effective multichannel approach is a must, since the better that collections departments get to know their customers, the more nuanced—and effective—the channel strategies they apply can be. The business case for doing this is compelling: the cost of going digital in collections will be a small fraction of the payoff in efficiency, effectiveness, and improved customer experience that the strategy creates.

**Matt Higginson** is a partner in McKinsey's Boston office, **Frédéric Jacques** is a partner in the Montréal office, and **Glen Kushta** is an analytics specialist in the New York office.

Copyright © 2019 McKinsey & Company. All rights reserved.

# What will Europe's ePrivacy Regulation mean for your business?

The ePrivacy Regulation, an elaboration of the GDPR, has been moving closer to adoption. Beyond preparing for compliance, smart companies can find business advantages.

*by Daniel Mikkelsen, Henning Soller, and Malin Strandell-Jansson*



© Laura Zulian Photography/Getty Images

**As companies continue** to scramble to implement the requirements of the European Union's 2018 General Data Protection Regulation (GDPR), another set of data-protection obligations has appeared on the horizon (for more on the GDPR, see "GDPR compliance since May 2018: A continuing challenge," on page 69). Europe's ePrivacy Regulation is in an advanced stage of preparation and is expected to replace the 2002 Privacy and Electronic Communications Directive (known as the ePrivacy Directive) by late 2019 or early 2020. Its focus is on privacy protection for data when they are transmitted electronically, and its status as a regulation (rather than a directive) means that it can be uniformly enforced across EU member states.

Many executives have not paid much attention to the new regulation, whether because it has yet to be enacted or they believe it will not apply to their businesses. In our view, the inattention is ill advised. In broad terms, the regulation specifies how the general data-protection framework outlined in the GDPR will be applied to electronic-communication services provided over telecom networks and the internet. The regulation will apply to direct marketing sent over electronic-communication networks, an activity most companies engage in. It will also apply to the providers of electronic-communication services—such as the presentation and retrieval of information on the internet—and to the providers of the software and directories that support these services.

In the making, the new regulation has been highly contentious and one of the most lobbied proposals in the history of the European Union. One concern is that the introduction of a regulation targeting a specific set of companies could put these companies at an unfair disadvantage to those not subject to this regulation. Another concern is that the provisions of the new regulation could come into conflict with those of the GDPR. EU member states have also expressed fears that the regulation could limit innovation.

Despite the controversy, most market analysts believe the regulation will be enacted, and any

company using electronic communications will have to monitor developments and prepare to meet the requirements. Penalties for infringement will be steep, with a top fine of 4 percent of worldwide revenues or €20 million, whichever is greater. In response, smart leaders will take a strategic view. They will work to help shape the new regulation and develop policies and practices to support compliance along the entire customer journey, especially in direct-marketing activities.

### **The key elements of the new regulation**

The new ePrivacy Regulation will repeal and replace the European Union's current ePrivacy Directive (exhibit). The new provisions will cover electronic-communication networks; data stored in or sent from end-user equipment such as phones, tablets, and computers (including cookies, device IDs, and other identification software); and methods employed to approach customers over electronic-communication networks for direct-marketing purposes.

The most important aspects of the new provisions are summarized as follows.

#### **Data processing**

The GDPR set out a list of general lawful purposes for data processing, namely vital interest, legal obligation, contractual necessity, legitimate business interest, public interest, and other purposes with the data subject's consent. While some of these purposes, such as the protection of vital and public interests (including statistical use and scientific research), are being considered for inclusion in the ePrivacy Regulation, the new regulation mainly takes a different approach. It will define specific requirements for different forms of usage.

For example, the use of cookies will require consent, except when the cookies are necessary for transmitting data, providing a requested service, or measuring a web audience. This means that all marketing-related cookies will require consent. Consent will also be required for metadata used in digital marketing, unless it is being used

## The European Union's uniformly enforceable ePrivacy Regulation will replace an older directive and augment the GDPR in protecting the privacy of data sent electronically.

Change	Current ePrivacy Directive	New ePrivacy Regulation
Automatically applies	Member states must adopt into law the 2002 directive for it to become applicable	New regulation is directly applicable and enforceable without being adopted into member-state law
Covers internet companies	Personal data are processed in connection with the provision of <b>publicly available electronic-communication services</b>	<b>Broader in scope</b> , including providers of electronic-communication networks or services
Covers metadata	<b>Covers communications data (including traffic data) but not metadata</b>	<b>Covers both content and metadata</b> , including cookies, online identifiers, search engines, directories, and direct marketing
Stricter cookie rules	<b>Customers must opt in</b> for information stored in the electronic-communication network or in terminal equipment (eg, cookies), except for transmitting or facilitating transmission, or if strictly necessary to provide a service explicitly requested by the user	<b>Consent is required throughout</b> , except for the provision of requested services, antifraud measures, security, software updates, or statistical purposes (eg, web-audience measuring)  Cookie settings should be allowed in the browser settings
Stricter rules on marketing calls	<b>Users have control</b> over line identifications, call blocking, and call forwarding  <b>Direct marketing is not allowed without consent</b> (B2C and B2B for member states to decide), except to existing customers; must <b>opt out from directories</b>	<b>Marketing calls must be clearly identifiable</b> as such, from the phone number or otherwise  <b>Consent is required for inclusion in directories</b> , barring a national exception
More efficient enforcement	<b>Enforcement at the national level</b> ; fines vary and are often rather low	<b>GDPR-specified uniform enforcement across member states</b> ; fines of up to 4% of worldwide revenue

for purposes related to service quality, billing, interconnection, or fraud prevention. In addition, the ePrivacy Regulation has stricter consent requirements than the GDPR. Under current plans, it will require companies to contact customers twice a year to remind them of their right to opt out or withdraw their consent, whereas the GDPR does not specify an opt-in/opt-out schedule.

If the new regulation is approved in its current state, its impact is likely to be significant. All major companies use cookies—whether their own or from a third party—to improve their marketing. Cookies

allow companies to target advertising to specific groups and analyze visitor traffic and behavior on their websites. According to a joint report from the Reuters Institute for the Study of Journalism and the University of Oxford, based on an analysis of 500 popular sites conducted in early 2018, more than 60 percent of websites had at least one third-party cookie per page; news sites had an average of 81 per page.<sup>1</sup> A subsequent study by the same team noted that the number of advertising and marketing cookies on news sites fell by 14 percent between April 2018 (before the GDPR was implemented) and July 2018 (shortly after implementation).<sup>2</sup>

<sup>1</sup> Rasmus Kleis Nielsen and Timothy Libert, *Third-party web content on EU news sites: Potential challenges and paths to privacy improvement*, a joint report from Reuters Institute for the Study of Journalism and University of Oxford, May 2018, [reutersinstitute.politics.ox.ac.uk](https://reutersinstitute.politics.ox.ac.uk).

<sup>2</sup> Lucas Graves, Rasmus Kleis Nielsen, and Timothy Libert, *Changes in third-party content on European news websites after GDPR*, a joint report from Reuters Institute for the Study of Journalism and University of Oxford, August 2018, [reutersinstitute.politics.ox.ac.uk](https://reutersinstitute.politics.ox.ac.uk).

### **Direct marketing**

Direct marketing via email and telephone also requires consent, unless contact takes place within an existing client relationship for a similar type of product. As before, companies need to offer customers an easy way to opt out of direct marketing every time they are approached. The regulation recommends that individual countries introduce “do not call” registers that companies must check before approaching individuals. It also requires that marketing calls use a specific prefix or code that makes them identifiable as such. Those making marketing calls must also identify the legal entity or individual on whose behalf they are calling.

### **Control and confidentiality of communications**

The ePrivacy Regulation strives to maintain individuals' control over communications through provisions that are broadly similar to those in the directive it is intended to replace. Individuals have the right to block certain numbers and be excluded from public directories. They can also decide on privacy settings for telephone, computer, and internet communications. Electronic communications in the form of data, metadata, and voice recordings need to be treated as confidential and cannot be disclosed without consent or the presence of a legal obligation. This also applies to machine-to-machine or Internet of Things communications over electronic networks, and to public Wi-Fi communications.

### **Integrating data privacy into corporate strategy**

All signs indicate that the new regulation will deepen the impact of the GDPR on most companies. The GDPR is already having a dramatic effect: our research indicates that marketing activities in Europe have declined by 10 percent since it was introduced. Some companies are struggling to address their existing customer base, with opt-in ratios of only 20 percent or lower. The ePrivacy Regulation will put even stricter rules in place.

Faced with such a challenging situation, companies need to address the new regulation with urgency while maintaining a strong focus on their business. To prepare for success under the new regulation, companies can consider taking the following actions.

#### **Set up a cross-functional team that involves marketing**

Marketing should be a key stakeholder in the implementation program. When programs are run by the legal or compliance function alone, they tend to focus purely on compliance. Cross-functional teams deliver the best results by looking for solutions that fit the company's overall business strategy as well as meeting customers' needs.

#### **Take an active role in developing the regulation**

Companies should engage in industry dialogue to assess the real-world impact of the provisions

**Cross-functional teams deliver the best results by looking for solutions that fit the company's overall business strategy as well as meeting customers' needs.**

and propose best-practice solutions to safeguard end-user privacy while also fostering innovation and market development. Online companies have already managed to secure the removal of a provision on preinstalled cookie settings in browsers that could have adversely affected business models based on online advertising. Leaders need to analyze the impact of the proposed regulation on their business and treat the need to safeguard data privacy as an opportunity to strengthen their branding and turn compliance investments into a form of strategic marketing. At the same time, they need to avoid taking steps that might incur unnecessary costs or hinder business development.

### **Optimize customer journeys to obtain consent to future contact**

Our experience suggests that low-involvement marketing methods such as direct mail and untargeted email campaigns rarely achieve opt-in rates above 20 percent. Such low levels of consent make it difficult for companies to engage with potential new customers or cross-sell to existing customers. However, opt-in rates can reach much higher levels with the right choice of consent strategy and formulation of consent notices. We have seen companies achieve rates as high as 80 to 90 percent by offering customers easy and convenient ways to opt in at every touchpoint along the customer journey and by making them feel they have something to gain from future contact.

### **Make privacy a competitive differentiator**

Privacy is a relative newcomer to top management's strategic agenda, so companies should seize the chance to evaluate what business opportunities the new requirements may create. For example, the right of portability, established under the GDPR, and the stricter control over direct marketing and directories could open up markets to competition and allow the development of new offerings in areas such as open banking, privacy and security solutions, comparison platforms, and intermediary services that help customers find a trusted provider or switch to a new provider. Marketing and legal departments can also work together to make privacy notices and consent requests stand out, not only to improve opt-in ratios, but also to enhance customer perceptions and support business building.

---

The ePrivacy Regulation about to come into force in Europe is part of a broader trend that is spreading to Asia, Latin America, and the United States. Successful companies not only will take timely steps to comply with the regulation but will also treat data privacy as an integral part of corporate strategy. By assessing the possible impact of the regulation, developing a clear and comprehensive road map for addressing it, and managing business implications carefully, companies can turn the regulation from a burden to an opportunity.

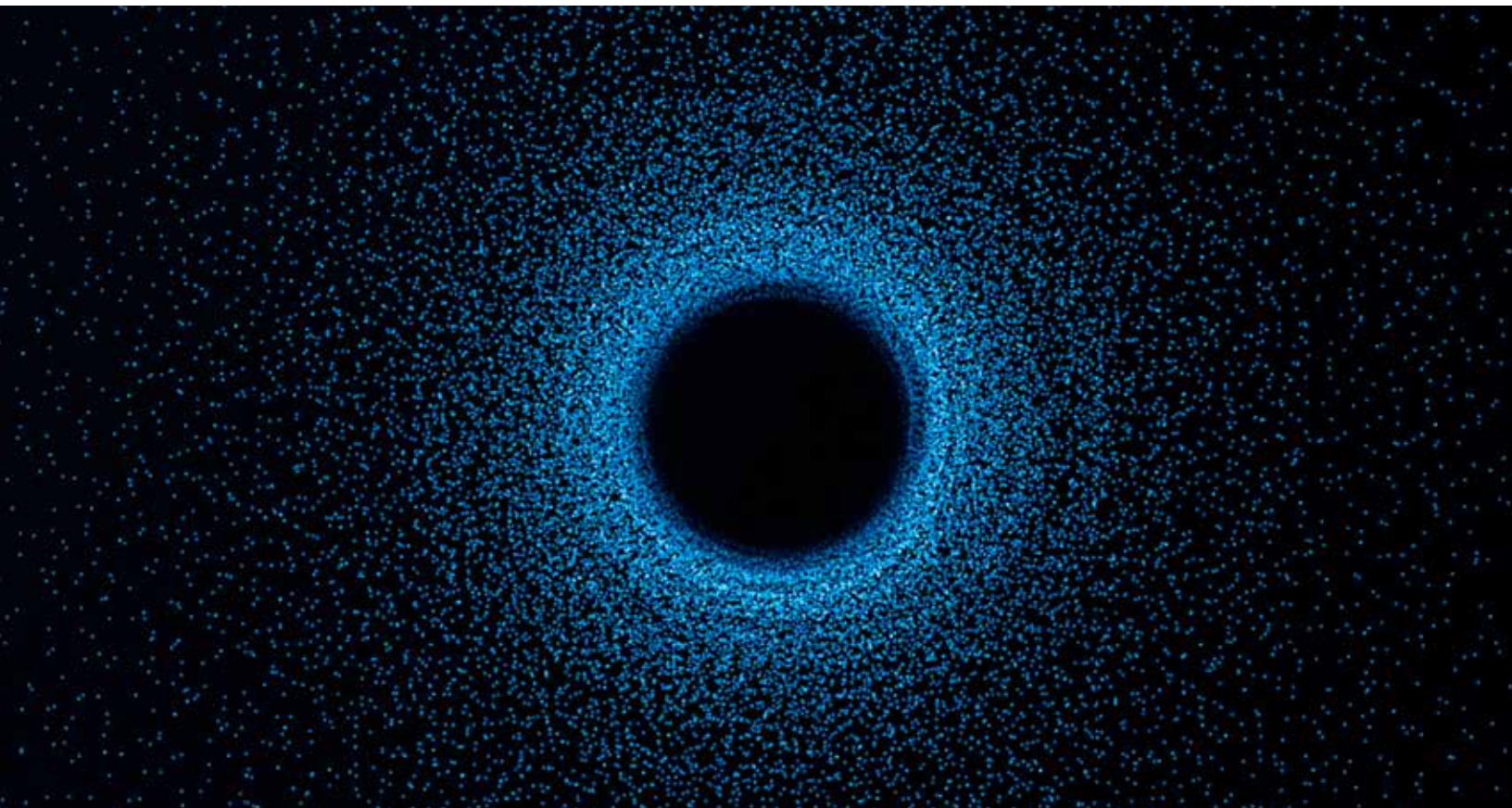
**Daniel Mikkelsen** is a senior partner in McKinsey's London office, **Henning Soller** is a partner in the Frankfurt office, and **Malin Strandell-Jansson** is a consultant in the Stockholm office.

Copyright © 2019 McKinsey & Company. All rights reserved.

# GDPR compliance since May 2018: A continuing challenge

Companies must automate and streamline, or the challenge of GDPR compliance will overwhelm them.

*by Daniel Mikkelsen, Henning Soller, Malin Strandell-Jansson, and Marie Wahlers*



© Rost-9D/Getty Images

**With the implementation** of the European Union's General Data Protection Regulation (GDPR) on May 25, 2018, a new regulatory regime for business in Europe and beyond has begun. McKinsey research shows that few companies feel fully compliant: as many as half, feeling at least somewhat unprepared for GDPR, are using temporary controls and manual processes to ensure compliance until they can implement more permanent solutions. Broader organizational challenges—particularly honoring and protecting the rights of data subjects and ensuring that impact assessments, reporting of breaches, and audit organizations are functioning properly—persist as well. With numerous stopgaps still in place, companies struggle to implement sustainable, long-term solutions.

### **GDPR's international reach**

While the GDPR is an EU regulation, it is not solely an EU matter. It has global reach, as GDPR obligations affect international companies with customers or employees in Europe as well as those serving as data processors in Europe or for European companies. Governments outside Europe are introducing new data-protection regulations or enhancing existing rules to make them similar to the GDPR. Recognizing the need to maintain a trusted and competitive digital environment, as well as to ensure free transfer of personal data to and from the European Union, places that have acted include Australia, Brazil, California in the United States, Japan, and South Korea.

### **IT implementation is still under way**

As we have seen, businesses continue to work on IT solutions for GDPR projects, many by using manual processes and temporary controls extensively to ensure compliance. Such measures, however, do not add up to a sustainable approach, especially given the regulatory requirements for the use of state-of-the-art data-protection technology, the likely

increase in requests for access to personal records over time, and the growing challenge of keeping personal data secure. Three areas need particular attention: security controls, data management, and automation.

### **Security controls**

Data-security breaches can tarnish a company's reputation and damage its finances, as recent major incidents at global organizations show. According to research by the Ponemon Institute, the average cost of a data breach in 2017 was \$3.62 million—or \$141 for each compromised record. Implementing security controls will probably account for the biggest share of future spending on the GDPR for most businesses.

To maintain robust data security, companies must implement IT controls in line with those of peers and adopt best practices in areas such as encryption, data anonymization or “pseudonymization,” and identity and access management. Companies should also base their investments on up-to-date appraisals of their security gaps in personal data. The controls themselves must reflect the content of the personal-data assets in question. A master customer-data system, for example, requires stricter controls and better protection than does a system containing security contacts for a business team.

### **Data management**

Manual processes and temporary work-arounds are prevalent in certain aspects of data management relevant to GDPR compliance.

#### *Responses to requests from data subjects exercising their rights under the GDPR.*

Customers may want to access their records—for example, to transfer their personal data to other institutions. Many companies approach such requests pragmatically by opting, for now, to use “centers of excellence.” Then such companies wait to see how many requests they receive



from customers before deciding which technical solutions to pursue in the long term. In a few cases, such as those involving the right of data subjects to access, automation has already been deployed. The solutions in use have not, however, matured enough to capture the full complexity of the requests expected under the new regulation.

***Transparency for customers, as encoded in fair-processing notices and consent statements.***

Transparency is crucial to ensure the fulfillment of formal requirements. One European regulator, for example, imposed a multimillion-dollar fine on one corporation for violating the GDPR's transparency standards. To offer customers an informed opt-in option while still managing to keep opt-in ratios reasonable, companies will need to ensure that consent-management systems are auditable and that consent statements are really transparent and well positioned.

***Reporting of data breaches.*** Only 25 percent of the companies we surveyed said that they can meet the requirement to report any data breach to regulators no later than 72 hours after management becomes aware of it. For a large, decentralized organization, reporting appropriately and quickly can be difficult. Companies will experience a sharp rise in mandatory interactions with regulators; according to estimates, the number of incidents that must be reported may increase 100-fold or more. To cope, companies will need to ensure that they have enough staff, adequate training, an appropriate process, and a ticket system that handles related requests.

**Automation**

Article 30 of the GDPR requires businesses to record processing activities that use personal data. So far, most companies have treated this as a mostly manual exercise, running surveys to capture data-processing activities and their characteristics. To keep the Article 30 record updated, however, companies will have to run such surveys regularly. Although full automation is unusual, companies can introduce automated tools to ease part of the burden.

To orchestrate the update of the Article 30 record, some businesses already use tools such as collaboration platforms that provide data-storage capabilities. What's more, tools that use artificial intelligence and business rules to identify personal data are now mature enough to help update the Article 30 record. Tools to identify data-processing activities and the personal data in them are starting to emerge and could eventually be adopted for this purpose as well.

**Organizational challenges remain**

The challenges companies have faced since May 2018 are not confined to data and IT. Businesses must also ensure that the processes designed during the preparations for the GDPR actually work and produce the expected results. Areas of particular concern include enabling the rights of data subjects, handling breaches and crises, and managing audit processes.

**Although full automation is unusual, companies can introduce automated tools to ease part of the burden.**

Unfortunately, the many companies that began their implementations late have not had sufficient time to pressure-test new processes and run “war games” on them. Adding to the complexity is the continuing uncertainty about the number and types of requests and breaches that may occur under the GDPR. In any case, the GDPR—and data protection in general—can be regarded, more and more, as strategic assets promoting the sustainable growth of companies.

At a time when individuals are becoming more aware of their rights and more concerned about the use of their personal data, companies must prepare for requests from a range of stakeholders: not just clients and regulators but interest groups and the media as well. Even compliant organizations run the risk of reputational damage if customers believe that they have not been treated fairly. Regulatory-reporting requirements and rising customer expectations also pressure companies to respond quickly when adverse events occur. This pressure is also reflected in the GDPR’s wide reach outside the European Economic Area and in the fact that regulators in other countries have adopted similar regimes.

For these reasons, we expect that many companies will continue to improve their GDPR compliance as part of wider efforts to streamline organizations and processes. Ideally, new IT solutions should be introduced only after internal testing and auditing. Data breaches or surges in requests may sometimes demand quick fixes, but the results are usually better if companies implement solutions in a more controlled way.

---

Companies will need to increase their level of automation and streamline the organization, or the challenge of sustaining GDPR compliance over the long term will overwhelm them. The important building blocks include support for tools, continued investment in cybersecurity, and improved internal processes. The lion’s share of investment in organizational and technical-security measures is still to come.

**Daniel Mikkelsen** is a senior partner in McKinsey’s London office; **Henning Soller** is a partner in the Frankfurt office, where **Marie Wahlers** is a specialist; and **Malin Strandell-Jansson** is a consultant in the Stockholm office.

Copyright © 2019 McKinsey & Company. All rights reserved.

**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, Risk Dynamics*  
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

## **In this issue**

Financial crime and fraud in the age of cybersecurity  
Flushing out the money launderers with better customer risk-rating models  
Scotiabank's chief risk officer on the state of anti-money laundering  
The risk-based approach to cybersecurity  
Cybersecurity: Linchpin of the digital enterprise  
Securing software as a service  
The customer mandate to digitize collections strategies  
What will Europe's ePrivacy Regulation mean for your business?  
GDPR compliance since May 2018: A continuing challenge

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

November 2019  
Designed by Global Editorial Services  
Copyright © McKinsey & Company  
McKinsey.com