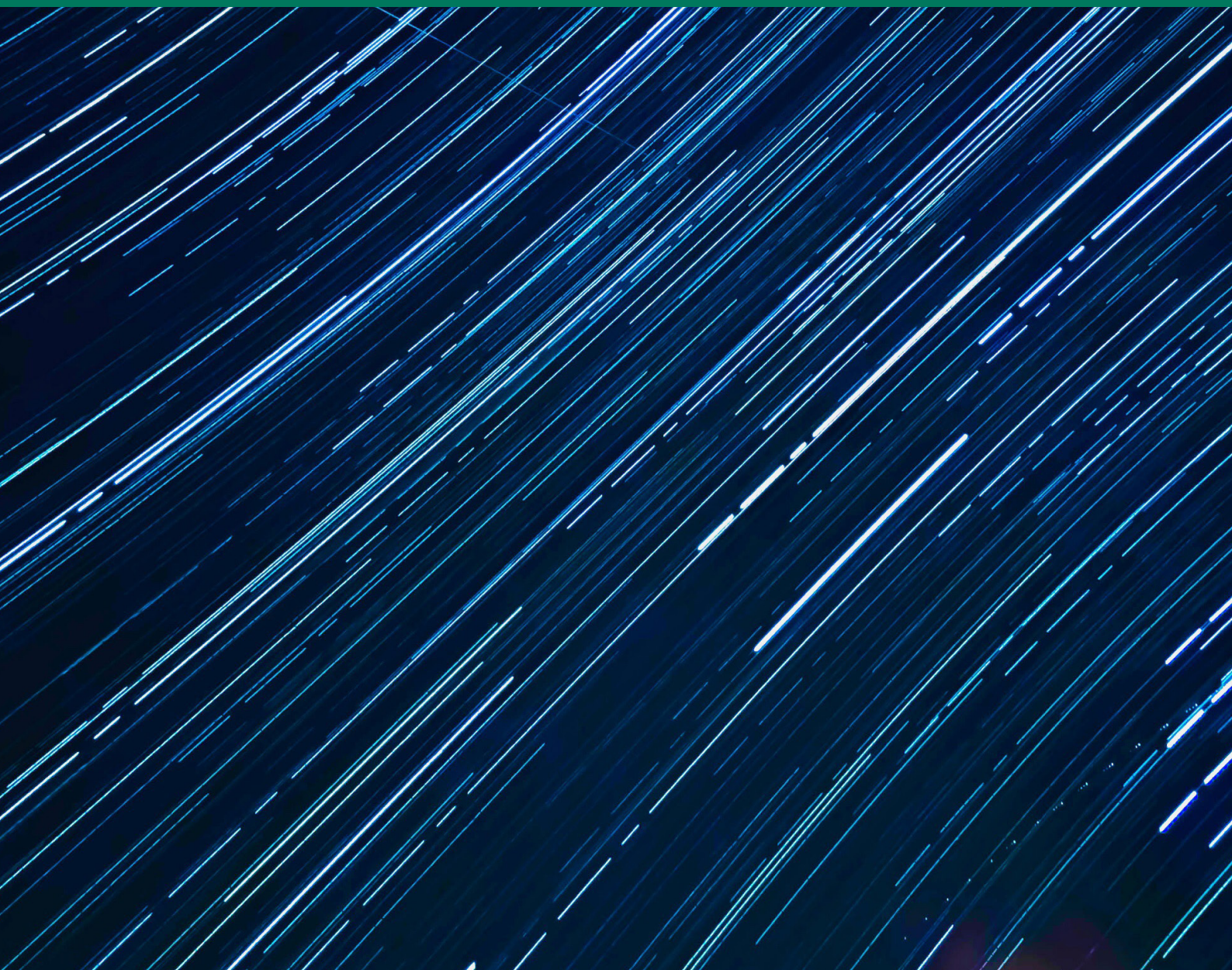
BCG

THE BOSTON CONSULTING GROUP

QuoScient

Banking's Cybersecurity Blind Spot—and How to Fix It



The Boston Consulting Group (BCG) is a global management consulting firm and the world's leading advisor on business strategy. We partner with clients from the private, public, and not-for-profit sectors in all regions to identify their highest-value opportunities, address their most critical challenges, and transform their enterprises. Our customized approach combines deep insight into the dynamics of companies and markets with close collaboration at all levels of the client organization. This ensures that our clients achieve sustainable competitive advantage, build more capable organizations, and secure lasting results. Founded in 1963, BCG is a private company with offices in more than 90 cities in 50 countries. For more information, please visit bcg.com.

QuoScient is a Frankfurt-based cyberdefense company. Our QuoLab social defense network and platform solves the core cyber problems of many companies: lack of security experts with enough operational experience, too many attacks, and a limited budget for cybersecurity. Our mission is to make clients safer with the resources they already have. QuoLab provides immediate orientation, decision making, and response capabilities, enabling teams to collaborate on investigations while ensuring data-privacy requirements are met at all stages of the defense life cycle.

BCG

THE BOSTON CONSULTING GROUP

QuoScient

Banking's Cybersecurity Blind Spot—and How to Fix It

Gerold Grasshoff, Walter Bohmayr, Marc Papritz, Jannik Leiendecker, Fabien Dombard, and Ioannis Bizimis

August 2018

AT A GLANCE

Information and IT security is a major concern for banks, their customers, and the wider financial system. Cyberattacks are now a daily occurrence, threatening billions of dollars of assets and the data of millions of customers. Executives understand that they need to act, but very few have a grip on the threat or an effective plan to respond.

Missing the Digital Threat

Too many banks have an information security blind spot. They lack a clear view of their key assets and don't see the threats in the digital shadows. Information and IT security is too often siloed in the IT function and does not receive enough senior management attention. Many banks still rely on perimeter defenses built over the past decade, which do nothing to frustrate clever attackers. A better approach is to accept the inevitability of a breach and focus on detection and response.

Building the Secure Banks of the Future

Banks must assess their risk tolerance and rebuild their operating models to reflect that assessment. Strategy, governance, risk management, IT architecture, and culture will likely need reinforcement. Once the new framework is in place, they must invest in platforms and operational capabilities to provide 24-hour protection. There will be a cost, but it will be low compared with the potential cost of doing nothing.

Cybersecurity is the most critical and immediate concern for banks, their customers, and the wider financial system. Financial institutions face a daily barrage of cyberattacks that can cause the loss of data, assets, and confidence, and as digital banking expands they are increasingly exposed. Still, many have no effective plan to respond.

The vast amount of customer data and financial assets held by banks makes them natural targets—nearly a quarter of all cyberattacks are directed at them. Adversaries from bedroom hackers to industrial spies and state actors have much to gain, and the cost of attack is low compared with the cost of defense. Incident rates are soaring. Last year, 50 UK financial institutions reported cyberattacks, compared with five just four years previously, according to the UK's Financial Conduct Authority.

A World Economic Forum report notes that cyberattacks are the most likely manmade threat facing the global economy.

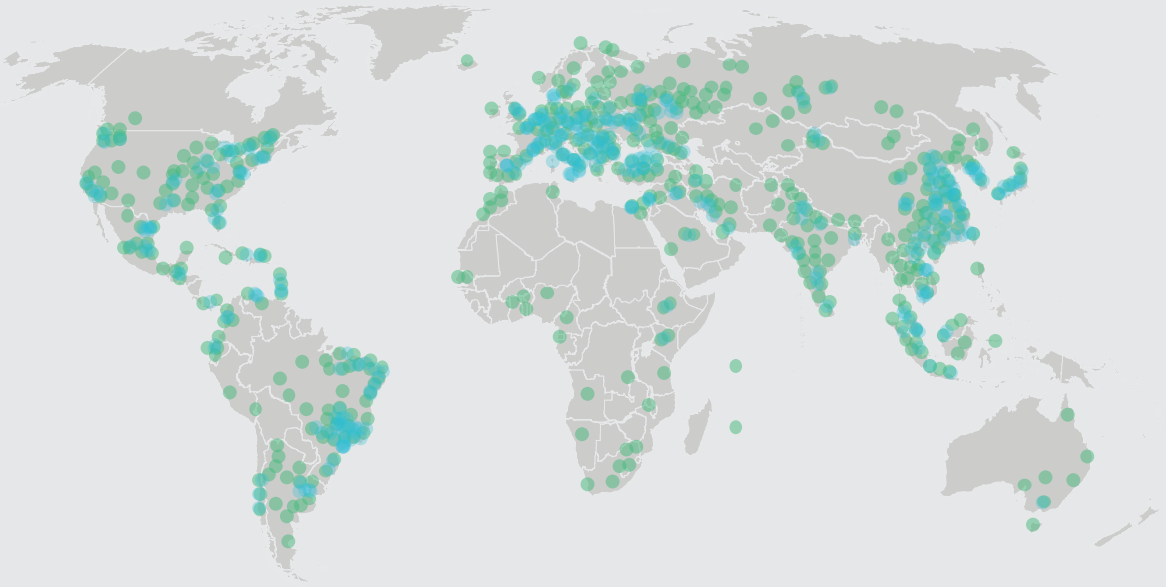
Despite the growing threat and increasing pressure from regulators to confront it, many banks have failed to engage cyber risk effectively, often treating it as a secondary concern. When they do investigate, it's not unusual to find intruders already inhabiting their systems. In the words of one expert, "Businesses fall into two categories: those that know they are being attacked and those that are being attacked but don't know it yet."

The most secure banks have ramped up their ability to detect and respond to attacks, but the majority require a strategic rethink. That means taking cybersecurity out of its IT silo and treating it as equal to risks such as credit, counterparty, and compliance. A new operating model is required, alongside strategic investment in talent, new technologies, and reformed ways of working throughout the organization. The task is complex, but the prize is valuable: a secure banking system for the digital age.

The Growing Information Security Threat

Cyberattacks are becoming more numerous, ambitious, and effective, with criminals regularly targeting payment systems, IT systems, and databases. (See Exhibit 1.) The vast majority of attacks go unreported, but numerous banks have been hit in the past year. In its most recent annual risk report, the World Economic Forum observed that cyberattacks are the most likely manmade risk facing the global economy, with data fraud/theft coming next. Not even central banks are immune. One of the most notorious recent incidents saw hackers take tens of millions of dollars from a central bank payment system.

EXHIBIT 1 | Cyberattacks Are Proliferating Worldwide



Source: QuoScient.
Note: The colored circles show the origin of all cyberattacks detected by QuoScient sensors on June 13, 2018, ranging from the smallest number (light green) to the largest number (dark blue).

Threats vary in style and intent. Distributed denial of service and payment system attacks are common, but attackers can also route through suppliers or seek to gain some advantage by taking private data hostage. More than 1,200 of these ransomware attacks were detected every day in 2017. Equal amounts of damage can be inflicted by disgruntled employees who publish confidential data on social media; likewise, damage can be accidentally self-inflicted, as a result of lost laptops or IT failures, for example. Estimates of annual losses across the industry run to the tens of billions of dollars.

The impacts of cybersecurity incidents go beyond the immediate loss of money or data. Clients and financial markets can quickly lose confidence, and the costs associated with repairing the damage and communicating with stakeholders are significant. In addition, the many digital touchpoints between financial institutions mean that contagion effects cannot be discounted, adding a systemic element to the risks banks face.

Regulatory Pressure Is Intensifying

Banks must respond to cybersecurity risk not only to protect their businesses but also to meet regulatory requirements and industry standards. Nearly three-quarters of jurisdictions worldwide are planning new cybersecurity regulations, guidance, or supervisory practices for the financial sector within the next year, according to the Financial Stability Board.

Among global examples, the ISO27k series of standards, published jointly by the International Organization for Standardization and the International Electrotechnical

Commission, provide best practices for information security management systems. They comprise recommendations regarding the processes, documents, technology, and people needed to manage, audit, and improve information security. Implementation requires board-level leadership and coordination.

Regionally, the European Union's General Data Protection Regulation, which went into effect in May 2018, aims to strengthen and unify data protection for individuals through stricter requirements on data confidentiality, identity, and access management. Fines for noncompliance can be as high as 4% of a company's annual turnover.

National authorities are also taking action. For example, the German banking supervisor (BaFin) in late 2017 published detailed banking supervisory requirements for domestic IT systems that focus on information security, including for outsourced products and services.

Among the many industry standards is SWIFT's Customer Security Program (CSP), which requires companies to protect and secure their local environment, prevent and detect fraud in commercial relationships, and share information. CSP comprises 27 control objectives for all institutions that handle SWIFT services, with self-attestations required annually.

Seven Weaknesses in Banks' Defenses

The increasing number and complexity of cyberattacks, alongside growing regulatory pressure, highlight the need for financial institutions to strengthen information security and cyber resilience. However, many are ill-equipped to respond to the challenge, in part because they have historically underestimated the risks. Their lack of preparedness has resulted in seven key weaknesses.

Limited Insight into Key IT Assets and the Threat Landscape. Banks often lack a defined process for assessing cyber risk, or they approach the exercise from back to front. The ideal starting point is to make a comprehensive inventory of data, applications, and networks and infrastructure. This can inform the next step, which is to specify the criticality of individual data sets. Criticality should be calibrated to the bank's protection goals related to confidentiality (some data is more valuable than other data), integrity (susceptibility to attack), and availability (what it will take to get back up and running after an attack).

Many banks are ill-equipped to respond to the growing cybersecurity threat, in part because they have historically underestimated the risks.

Banks must use the information they garner on data to determine where they are most exposed. At this stage, they often make the mistake of prioritizing applications and infrastructure, skipping the crucial first data step. Without a structured approach, banks can fail to gain a comprehensive picture.

The other commonly missing piece of the puzzle is an understanding of threats and how these might manifest (for example, through unpatched vulnerabilities on phones). Banks often rely entirely on newsletters and updates from security vendors to stay up to date, rather than performing an ongoing independent investigation into where they may be most vulnerable.

Failure to Prioritize Cybersecurity. Banks often fail to make cybersecurity a core element of the decision-making process in managing key IT assets. Often this is evidenced by the peripheral role of chief information security officers (CISOs), who may be disconnected from IT product development, digitization efforts, and operations. Banks tend to lack protocols for CISOs to assess concepts or provide feedback that would hardwire information and IT security awareness into the design or purchasing process. Too often they are out of the loop on board-level decisions and the proceedings of risk committees, or they are hobbled by a lack of adequate human or financial resources.

Focus on Prevention Over Detection and Response. Financial institutions habitually focus on preventing cyberattackers from entering their systems, which is useful in protecting against untargeted attacks but insufficient to secure the organization from determined assailants. The uncomfortable reality is that attackers are gaining entry with relative ease and are usually able to sit undetected in bank systems for long periods—an average of 200 days, according to one study.

Attackers are gaining entry to bank systems with relative ease and are usually able to sit undetected for long periods—an average of 200 days.

Given the practical impossibility of impermeability, the state of the art in information security has moved toward detection and response. However, those components are often missing from banks' risk management frameworks, which can lead to an insufficient allocation of resources and significant unmanaged risks.

Failure to Hire Talent. Financial institutions often fail to attract and retain enough people with the knowledge necessary to tackle threats and sustain operational capabilities. In a recent study, a German industry group focused on IT found that the number of unfilled positions in Germany rose from about 6,000 in 2014 to about 9,000 in 2016, a deficit the group predicted would widen. Adding to the staffing challenge facing financial institutions: the younger, more dynamic cohort associated with the cyber and IT community no longer sees finance as a natural career choice.

Weak Third-Party Management. Banks are increasingly turning to outsourcing to acquire and manage IT assets and control costs. According to one central bank estimate, the percentage of outsourced services in bank IT budgets increased to 42% in 2017, from 36% five years before. The security of services provided by outsourced contracts, including cloud hosting, remains the responsibility of the bank. However, many banks do not know how their IT partners work and few have in place systems and protocols for oversight and monitoring. Banks do not have the resources to police every vendor they work with or to monitor external vulnerabilities and networks.

Lack of a Security-Aware Culture. Many banks lack a culture in which the institution as a whole (including risk owners, risk managers, and audit) takes responsibility for reducing information security risk, encouraging collaboration, and building systemic resilience. Often information security is the sole responsibility of the CISO, and there is insufficient leadership, awareness, and expertise at the board level. Banks commonly fail to provide their staffs role models, training, tools, or incentives. Employee negligence and malicious acts account for two-thirds of cyber breaches, while less than 20% are directly driven by an external threat, according to a 2017 analysis by advisory firm Willis Towers Watson.

Operational Stress. Amid an accelerating rate of attacks and incidents, banks' organizational capabilities come under extreme pressure, often leading to systemic breakdowns and accumulating backlogs. Operational shortfalls can include weak knowledge resources, a lack of codified processes to manage incidents (resulting in heterogeneous responses), and insufficient technology to monitor, log, and react to suspicious activity. A common problem is an inability to integrate technology and human capabilities. The result is operational inefficiency, more risk, and a lack of the resources needed to bounce back from a major incident.

What Banks Should Do Next

In the face of accelerating threats, banks must ramp up information security, building systems that enable speedy identification and resolution of breaches. We recommend a three-step approach, which includes: performing a comprehensive health check to assess cybersecurity maturity and available capabilities and prioritize activities; building a new operating model that manages development and implementation of strategy, governance and organization, risk management, IT, and culture; and ramping up operational capabilities to ensure continuing protection.

Perform A Comprehensive Health Check

A questionnaire provided to the CISO and to the IT and risk functions (among others) should cover all security aspects of the existing operating model. The questionnaire may be accompanied by document reviews, all aimed at determining the maturity of the firm's information security apparatus.

Banks should also create a threat profile, comprising a view of activities by industry, product, and geography, that aims to align threats with day-to-day operations and areas of specialization. If, for example, a bank has a strong payments franchise, it can focus its cybersecurity expertise on that activity. Banks should then conduct a threat-hunting exercise, in which they seek to identify attackers by, for example, scanning the dark web or by using sensors in internal systems.

A common problem is an inability to integrate technology and human capabilities, resulting in operational inefficiency and more risk.

Build A New Cybersecurity Operating Model

There is little value in an approach geared to isolated incidents or regulatory findings. Instead, banks must holistically rethink their organizational capabilities. That means instituting a dedicated operating model and providing CISOs and executives with a framework for information security risk management. (See Exhibit 2.)

The central goal of the new operating model should be the ability to reliably prevent attacks, detect intruders, implement a response, and carry out a recovery plan that includes communicating with stakeholders. In addition, the model must inform daily operational capabilities so that cyber risk is managed through a single strategic and operational approach. It is also crucial for banks to take cybersecurity out of its IT silo, treating it as equal to other key risks and making it subject to similar levels of analysis, modeling, and management.

The model should address strategy, governance and organization, risk management, risk architecture, and culture.

EXHIBIT 2 | Key Elements of a Cybersecurity Operating Model

Sources: QuoScient; BCG analysis.

Risk Strategy. Banks must start by defining the risks they face, establishing a taxonomy tailored to their business activities, assets, and risk profile. Executives should be able to quantify how much risk the bank can tolerate in view of its key assets.

Governance and Organization. Banks should erect governance frameworks for the management of information risk across the three lines of defense: risk owners (business lines and IT), risk management (including the CISO and risk committees), and internal audit. The organizational model should reflect the crucial role and responsibilities of the CISO, who must have sufficient power to represent information security issues across business lines and decision-making hierarchies. The CISO should be largely independent from the IT function and have a sufficient budget.

Given the difficulty of obtaining and retaining talent and operational capabilities, banks must balance employee training and development against the likelihood that internal capabilities will be insufficient in the short term. External advisors and vendors can be useful in keeping banks informed of the evolving threat landscape and in day-to-day monitoring, but banks need to be smart about marrying them to internal teams and work toward long-term self-sufficiency.

Risk Management. Banks should conduct regular assessments of regulatory requirements across jurisdictions and ensure that these are reflected in their own policies, procedures, and guidelines. They should implement monitoring processes in order to be kept up to date.

Risk assessment—mapping key IT assets to threats—is crucial. Banks must evaluate their internal controls and make a risk treatment decision; there are four choices: accept the risk (do nothing), mitigate it, avoid it (close the relevant business or system), or transfer the risk (through insurance).

From an operational perspective, risk management requires the ability to detect and observe intruders, usually by analyzing system sensors and databases. One approach is to identify anomalies in log-in data—for example, a system user appearing to log in while on vacation or at other unusual times. The bank must have a regularly rehearsed response-and-recovery plan ready when an intruder is detected or some other breach occurs (even something as minor as a lost laptop). There should be an accompanying communication strategy, both internal and external (including for regulators). In the recovery phase, forensic examination of the incident is key to reinforcing defenses.

In relation to outsourced IT contracts, banks must put in place governance and protocols for oversight and monitoring, which may be automated. Contracts should be reviewed and aligned with the new operating model.

Risk Architecture. Getting the architecture right is about making the strategy real in the bank's data/information, applications, and networks and infrastructure. CISOs should trigger implementation programs—guiding IT teams to harden systems, for example, by requiring more complex passwords that must be renewed more often—and make standards an integral part of application development. One imperative is to ensure that risk policies are understood by stakeholders and are properly incorporated into systems. Regulatory compliance and processes should also be monitored.

Banks must have a regularly rehearsed response-and-recovery plan ready when an intruder is detected or some other breach occurs.

Culture. The tone from the top is crucial in creating a cybersecurity mentality and promoting information sharing, with senior management actively highlighting the need for reinforced information security. Banks should also embrace the sharing of information on threats and incidents, both internally and with peers and third parties. In the words of one expert: "Detection by one party can be prevention by another."

Ramp Up Operational Capabilities

Implementing a reformed operating model and integrating new human capabilities and technology present significant challenges. There is a vast array of tools available on the market, but often banks choose too many, creating a fragmented defense. This can lead to gaps in oversight and extended "dwell times" between when a bank is compromised and when the compromise is detected. A single platform is preferable, designed to provide a real-time consolidated view.

A smart technology stack, supported by machine learning to improve mechanisms over time, should be deployed to integrate diverse security controls and platforms.

Machine learning also helps reduce noise by distinguishing between real alerts and false positives. Integrated systems can conduct continuous sweeps across the bank's IT data, applications, and network and infrastructure, interrogating databases in search of anomalies.

The transformation to operational excellence can be characterized as a journey from preincident measures, such as antivirus software, to threat intelligence and rapid response and finally to forensic analysis. It should be supported by a dedicated security operations team and subject matter experts, or "special forces," to drive defense operations and strategy. When an incident occurs, the critical asset is time, and these experts should be mandated to respond quickly and autonomously.

BANKS ARE UNDER almost constant assault from cyberattackers, but many lack the operational capabilities and resilience that would provide adequate protection. They have limited insight into their key assets and little understanding of the threats they face. A shortage of talent exacerbates the challenges. Executives must take steps to face the threat to consumers, to banks themselves, and to the stability of the financial system. That means recognizing that cyber risk is more than just an IT problem, but rather a primary risk of the banking business. They must respond strategically and operationally, starting with a health check and moving to embed cyber resilience into the operating model. At the same time, they should add the technology and staff needed to monitor, detect, and respond to attackers on a daily basis. In the coming era of digital banking and ecosystems, cyber threats will grow and accelerate. To preempt the onslaught, the time to act is now.

About the Authors

Gerold Grasshoff is a senior partner and managing director in the Frankfurt office of The Boston Consulting Group and global head of risk management and regulation and compliance. You may contact him by email at grasshoff.gerold@bcg.com.

Walter Bohmayr is a senior partner and managing director in the firm's Vienna office and global head of cybersecurity. You may contact him by email at bohmayr.walter@bcg.com.

Marc Papritz is a partner and managing director in BCG's Düsseldorf office. You may contact him by email at papritz.marc@bcg.com.

Jannik Leiendecker is a principal in the firm's Munich office. You may contact him by email at leiendecker.jannik@bcg.com.

Fabien Dombard is cofounder and CEO of QuoScient. You may contact him by email at fabien.dombard@quoscient.io.

Ioannis Bizimis is cofounder and COO of QuoScient. You may contact him by email at ioannis.bizimis@quoscient.io.

For Further Contact

If you would like to discuss this report, please contact one of the authors.

To find the latest BCG content and register to receive e-alerts on this topic or others, please visit bcg.com.

Follow The Boston Consulting Group on Facebook and Twitter.

8/18


BCG
THE BOSTON CONSULTING GROUP


QuoScient