

White Paper

Innovation-Driven Cyber-Risk to Customer Data in Financial Services

Prepared in collaboration with Oliver Wyman



Contents

- 3 Executive summary
- 4 Introduction and approach
- 5 Stage 1: Identifying challenges
- 8 Stage 2: Designing solutions
- 10 Stage 3: Prioritizing solutions
- 12 Conclusion
- 13 Appendix
- 17 References
- 18 Acknowledgements

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
Email: contact@weforum.org
www.weforum.org

World Economic Forum®

© 2017 – All rights reserved.
No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying and recording, or by any information storage and retrieval system.

The views expressed in this White Paper are those of the author(s) and do not necessarily represent the views of the World Economic Forum or its Members and Partners. White Papers are submitted to the World Economic Forum as contributions to its insight areas and interactions, and the Forum makes the final decision on the publication of the White Paper. White Papers describe research in progress by the author(s) and are published to elicit comments and further debate.

Executive summary

As businesses rely more on technology and amass larger stores of data, protecting customer information has become increasingly important to maintaining a secure and trusted financial services system.

However, technology-driven innovations – from digitization and application programming interfaces (APIs) to robotics and biometrics – are expanding the amount of customer data at risk as well as enabling more sophisticated cyber-attacks.

The financial services system faces challenges, both internal and external, in managing innovation-driven cyber-risk. Internally, challenges around technology and expertise; externally, challenges around coordination with regulators and across the industry.

The solutions described in this report were developed using a rigorous three-stage process to identify cyber-risk challenges, and to design and prioritize solutions. They are based on extensive research, interviews with more than 30 subject matter experts, and the project Steering Committee and Working Group meetings.

Of the 19 solutions identified to address innovation-driven cyber-risk to customer data, two have been prioritized for further action by the World Economic Forum project team. The 17 additional solutions are strongly recommended for consideration by actors across the financial services system.

- **Cyber-risk measurement:** Advanced approaches and standardized measures for cyber-risk quantification are needed to improve the understanding and comparability of cyber metrics and help organizations maximize the return on their investments.
- **Cybersecurity assessment:** Enhanced cybersecurity guidance and assessment mechanisms, including common principles for cybersecurity assessments, a point-based scoring mechanism and practical steps for improvement, will allow companies to evaluate and improve their cybersecurity readiness.

The framework described in this white paper provides a toolkit to identify cyber-risk management improvements in an innovative and fast-changing environment through public-private partnerships. In addition, the identified solutions offer concrete examples of how the framework can be applied in practice.

This document builds on the **Balancing Financial Stability, Innovation and Economic Growth** white paper published in June 2017, which identified the following findings:

1. **Major innovation-driven change is coming to financial services.** Firms are increasingly competing or partnering at different points along the financial services value chain to take advantage of unmet customer needs, less efficient cost structures, high capital usage and attractive returns.
2. **These changes can bring enormous benefits to the financial services system,** including improved customer experience, better risk management, greater efficiency for incumbent industry participants and new value creators.
3. **Managing some systemic risks introduced by this wave of innovation poses challenges.** In particular, cyber-risk was identified as perhaps the single most important risk to the current financial services system.
4. **The financial services system would benefit from certain tools to achieve greater enablement and risk management,** such as an improved mechanism for public private cooperation to prevent cyber-attacks.

Introduction and approach

A rigorous three-stage process was used to identify innovation-driven cyber-risk challenges, and to design and prioritize solutions. The solutions described in this document are based on extensive research, interviews with more than 30 subject matter experts, and the project Working Group and Steering Committee meetings.

Stage 1: Identifying challenges. The starting point was a forward-looking set of innovations with potential to transform the financial services system's cyber-attack surface. These innovations were evaluated for their impact on cyber-risk through interviews with more than 30 subject matter experts.

Stage 2: Designing solutions. Based on this impact assessment, the solution space was designed as a matrix of cyber-risk management lifecycle stages and implementation mechanisms. The cyber-risk management lifecycle stages are based on the National Institute of Standards and Technology (NIST) framework, and address how companies can understand their cyber-risks, protect their attack surfaces and recover after a cyber-attack. The implementation mechanisms focus on how solutions would be operationalized, whether through principles, regulation, partnerships, or outsourcing. For each intersection not covered by existing industry initiatives, innovative solutions were identified through research, interviews, comparison to other industries and adaptation of existing solutions.

Stage 3: Prioritizing solutions. Prioritization criteria were then applied by the project Steering Committee and Working Group to filter the solutions and ultimately derive a set of two concrete and actionable initiatives best suited for action through the World Economic Forum platform.

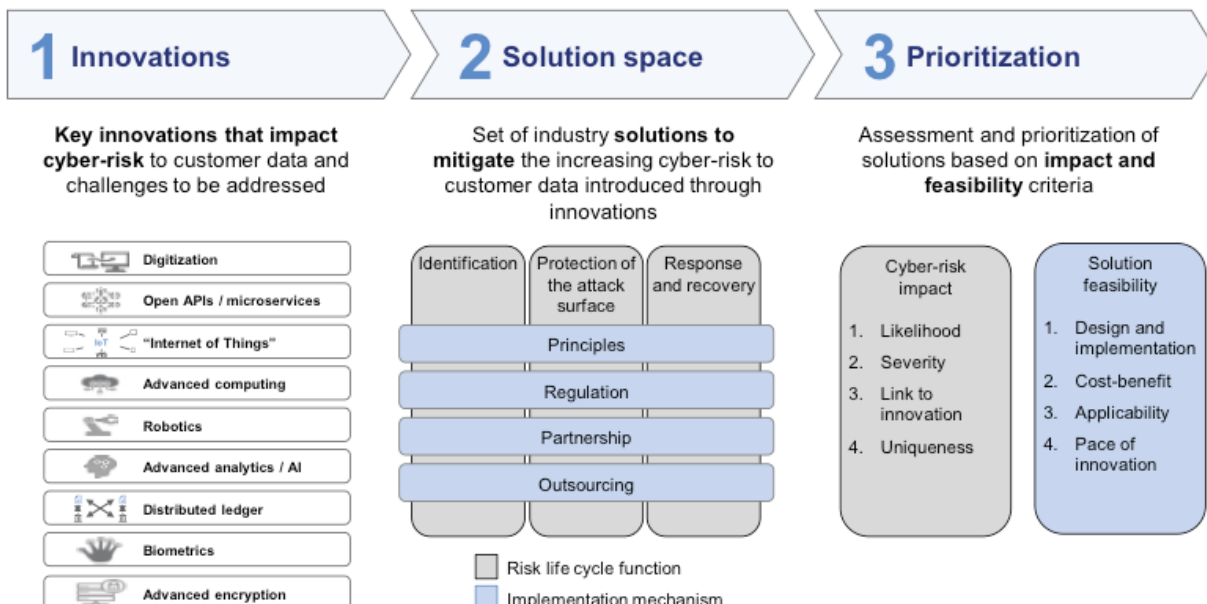


Cyber risk is a large and rapidly expanding subject, of critical importance to the financial system. The way forward involves breaking cyber risk down into more granular components, and developing practical risk management practices and solutions at that granular level. This report offers a solid step in that direction.



Stephen S. Poloz, Governor of the Bank of Canada

Figure 1: Approach to identifying a prioritized set of cyber-risk solutions



Stage 1: Identifying challenges

The financial services system faces three main challenges in protecting customer data from innovation-driven cyber-risk.

1. Innovation is increasing cyber-risk to customer data
2. Financial services firms face specific challenges in managing cyber-risk
3. Strategic, innovative, multistakeholder solutions are needed to address fast-changing cyber-threats

Innovation is increasing cyber-risk to customer data

Innovation is having a transformative effect on financial services. Companies are innovating faster in an effort to transform customer experience, and improve efficiency and effectiveness.

Technological advancements continue to build on each other, and are available to a broader audience to address increasingly complicated problems. In addition, increased interactions with innovative technologies have desensitized customers and workers to sound data security practices.

Technology-driven innovations, as shown in Figure 2, have the potential to increase cyber-risk to data in several ways:

- **Collection of data:** Innovations around the Internet of Things incentivize and facilitate the collection of large amounts of data. Growth in the volume, variety and concentration of data may increase its value as a target for cyber-attacks.
- **Sharing of data:** Innovations around open API/micro-services enable companies to transfer and share data more easily. Increasing the interconnectedness and velocity of data increases vulnerabilities by widening the attack surface, often to include less sophisticated actors.
- **Attack sophistication:** Innovations like artificial intelligence and machine learning support the development of more sophisticated cyber-attack capabilities. Increasing sophistication of attack capabilities also changes and intensifies the potential impact on data (e.g. manipulation of data, weaponization of data). Commodities of scale and the growing ubiquity of modular tools may also remove barriers for less sophisticated actors to perform malicious acts.



More than ever before we see the intersection of technology, innovation and business generating both opportunities and risks. This report highlights possible solutions, including the need for a coordinated, collaborative approach across multiple industries and government to address systemic issues.












Gavin Patterson, Chief Executive Officer, BT Group, United Kingdom

The amount of Internet of Things devices connected to IP networks will be three times as high as the global population in 2021.¹

The direct cost from cyber-security breaches can be expected to grow from \$1.7 billion in 2015 to more than \$6.8 billion by 2020.²

1. Cisco, Cisco Global Cloud Index: Forecast and Methodology, 2016–2021, 2017.
2. Marsh & McLennan, MMC Cyber Handbook 2018: Perspectives on the next wave of cyber, 2017.

Figure 2 Key technology innovations that impact cyber-risk to customer data

Technology	Description	
	Digitization	Digitization of customer information allows for housing all relevant information about a customer, including contracts and addresses. Digital interface with the customer allows for accelerated information exchange and facilitation of various processes
	Open APIs/ microservices	Publicly available application programming interface that provides developers with programmatic access to a proprietary software application or web service; architectural style that structures an application as a collection of loosely coupled services
	Internet of Things	Network of internet-connected objects able to collect and exchange data using embedded sensors, including autonomous/unmanned vehicles that can collect and distribute information
	Advanced computing (quantum, edge, cloud, mobile)	Includes network of remote servers hosted on the internet to store, manage and process data, rather than a local server or personal computer, as well as systems based on quantum effects, devices created using mobile components and/or optimization through performing data processing at the edge of the network (e.g. technologies that reduce timing dependencies when transferring data)
	Robotics	Software solutions that act as a virtual workforce to automate processes that are routine, repetitive, or rule-based
	Advanced analytics/ artificial intelligence	Statistics and modeling used to determine future performance based on current and historical data, including the ability to aggregate data from a variety of different sources
	Distributed ledger technology (blockchain)	A database that is consensually shared and synchronized across networks spread across multiple sites, institutions, or geographies, allowing transactions to have public "witnesses"
	Biometrics	Identity authentication through use of unique physical or behavioural characteristics, such as facial recognition, fingerprints, voice recognition, or unique digital identifiers
	Advanced encryption	Advanced encryption methods, such as zero knowledge proofs and tokenization of data, which disguise data in a more secure form

Financial services firms face specific challenges in managing cyber-risk

Technology

Cybersecurity professionals face structural disadvantages compared to cyber-attackers. Given the speed of innovation, it can be easier to leverage new technologies to attack a system than to protect an expanding attack surface. Many companies, particularly incumbents, also have legacy systems that may be more vulnerable to cyber-attack. Newer is not always better, however, as organizations can also face challenges around ensuring the security of new software programmes, particularly those created by third parties.

Expertise

Effective cyber-risk management requires both technical and operational expertise across all levels of an organization. However, management and boards currently have limited tools to assess and quantify cyber-risk. This applies equally to the third parties the organization relies on to deliver its services. There is also an insufficient supply of cybersecurity talent compared to growing demand for skilled workers, as well as a limited number of high-quality training programmes. Finally, customers have limited awareness of cybersecurity best practices and often fail to meet basic standards.

Oversight

Given the accelerating pace of innovation, there will necessarily be a lag in the ability of regulators to respond to technical and industry dynamics. While it is unrealistic for regulation to fully keep up with new technologies, the existing fragmentation of regulatory authority poses significant challenges for the financial services system. Beyond fragmentation, there are also gaps that exist in the oversight of non-incumbents and third parties with access to customer data. This is particularly important as customers and employees become more comfortable with new technologies, and desensitized to sound data security processes.

Collaboration

There has been a proliferation of cybersecurity frameworks and industry-led initiatives; however, most are uncoordinated and inconsistent. This may be partially driven by the fact that some companies may see cybersecurity as a competitive advantage. Many companies, particularly multinationals, must also consider the geopolitical implications of their cybersecurity decisions, which may limit cooperation.

Strategic, innovative, multistakeholder solutions are needed to address fast changing cyber-threats

Cyber-risk is not just a technology problem. Customer data plays an increasing role in the overall strategy for financial services companies, and data security requires a wide range of capabilities, people and processes. This paper therefore focuses on solutions that are strategic in nature, rather than purely technical.

Innovation creates opportunities, but it also poses risks. In many cases, it may be difficult to counter risks without leveraging new technologies to do so. For example, artificial intelligence can be used to increase the effectiveness of cyber-attack protections, including real-time learning against new threats. However, the same artificial intelligence tools can also be used by cyber-attackers themselves. Where possible, this paper also focuses on solutions that leverage the same innovations that may drive new cyber-risks.

Finally, given that many of the key cyber-risk challenges to financial services involve effective collaboration, it is logical that solutions will require the cooperation and resources of multiple actors. Incumbent banks and insurers must tackle the challenges of their legacy architecture and safely manage the shift towards working with new partners. New entrants, including technology firms and fintechs, must ensure they are adhering to cyber-security standards and making needed investments. Finally, supervisors and regulators must keep up with the pace of change, design effective regulation, and act as a point of communication with the private sector. The solutions considered leverage collaboration within and between public- and private-sector stakeholders, including joint industry initiatives and public-private partnerships.



The digital revolution impacting so many industries is reshaping how people all over the world shop, bank and invest. As the payment environment grows ever more complex and interconnected, security and trust are more important than ever. Malicious actors see this new world as a world full of opportunity; whereas we see it as our responsibility to stay ahead of cybercrime and protect our consumers, banks and merchants.



Ellen Richey, Vice-Chairman and Chief Risk Officer, Visa, USA

Stage 2: Designing solutions

Given the nature of the cyber-risk challenges described in the previous section, solutions needed to incentivize collaboration, either within or across the public and private sectors, and be distinct from existing initiatives.¹ Solutions also needed to be sustainable, and propose blueprint directives and standards rather than specific and prescriptive technical innovations.

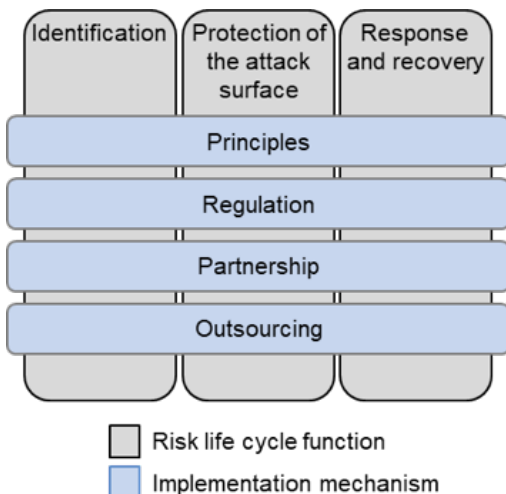
Solution dimensions

Solutions were dimensioned using the cyber-risk management lifecycle and across several implementation mechanisms.

The NIST framework was leveraged for the cyber-risk management lifecycle stages: identification, protection of the attack surface, and response and recovery. Identification focuses on how an organization understands its cyber-risks and prioritizes its risk-management efforts. Protection addresses the ability of an organization to limit or contain the impact of a potential cybersecurity event. Finally, response and recovery covers the ability of an organization to contain a cybersecurity event and return to normal operations.

Implementation mechanisms were divided into four approaches: principles, where institutions agree to abide by certain security principles; regulation, where regulators impose industry standards; partnership, where institutions contribute resources toward common solutions; and outsourcing, where services are provided through the use of a mandatory, independent third party.

Figure 3 Solution space dimensions



Cyber-risk solutions

Nineteen solutions were designed within nine categories as shown in Figure 4. Additional detail on each solution, including the challenge it was developed to address, can be found in the appendix.

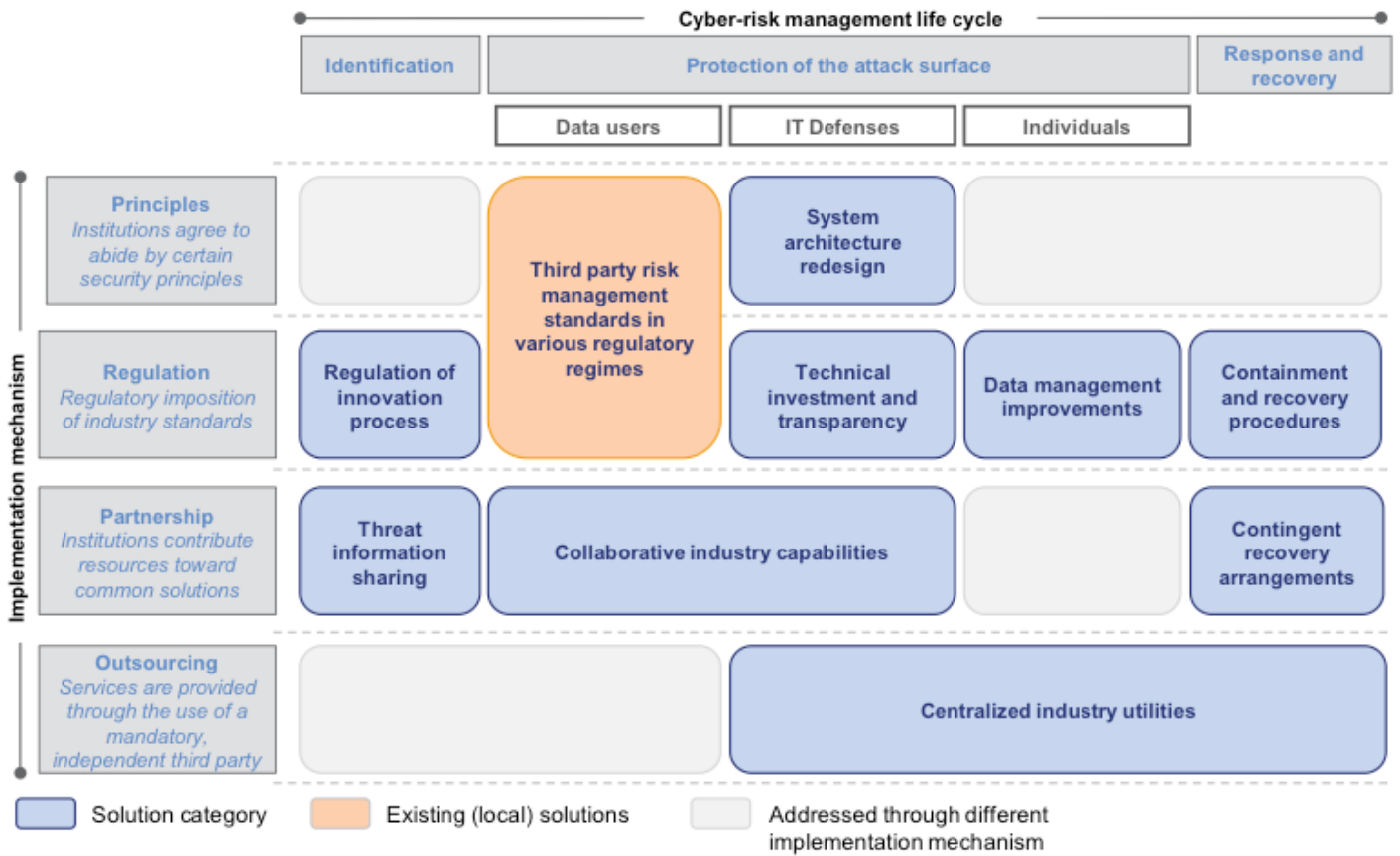
There are several areas of the solution set where solutions are not identified. This is for one of two reasons: either there are existing solutions for this area, or the area should be addressed through a different implementation mechanism.

“
At the core of cybersecurity is a culture of cyber-risk awareness. Cyber-risk awareness should pervade every aspect of an organization – its people, its processes and its technology.
”

Benoît Cœuré, Member of the Executive Board, European Central Bank, Frankfurt

1. Solutions are considered distinct if they have materially different content, or scale from existing initiatives

Figure 4: Cyber-risk solution categories



Stage 3: Prioritizing solutions

A rigorous set of criteria was used to evaluate and prioritize each of the nineteen solutions. Leveraging this assessment, two solutions were recommended for further action by the World Economic Forum project team. These solutions, cyber-risk metrics and a cybersecurity assessment, are described in detail on the following pages. Impact and feasibility considerations for each of the 19 solutions can also be found in the appendix. These solutions are strongly recommended for consideration by other actors across the financial services system.

Prioritization approach

Each solution was evaluated based on the criteria described in Figure 5: the impact of the solution on innovation-driven cyber-risk, and the feasibility of implementing the solution.

Impact criteria focused on likelihood and severity, as represented in the ability of the solution to reduce the

probability or potential consequences of a cyber-attack to customer data. How much the solution would address “innovation-driven” cyber-risk, as opposed to overall cyber-risk resilience, was used as a third standard. Finally, uniqueness was used as a way to identify solutions that have not yet been adopted in financial services and could have an outsized impact.

Feasibility criteria focused on design and implementation considerations, including the ability to overcome obstacles and drive adoption of the solution. Return on investment (e.g. cost-benefit) of the solution was also considered, as well as the ability to tailor the solution to different types of financial services institutions. The effects the solution could have on the pace of future financial services innovations was used as a final standard.

Figure 5: Solution assessment criteria

Cyber-risk impact

1. **Likelihood:** The degree to which the solution reduces the probability/frequency of a cyber-attack to customer data for the system
2. **Severity:** The degree to which the solution reduces the potential consequences of a cyber- attack on customer data for the system
3. **Link to innovation:** The degree to which the solution addresses “innovation-driven cyber-risk” versus general system resilience
4. **Uniqueness:** The degree to which the solution differs from solutions/initiatives already being pursued in the financial services industry

Solution feasibility

1. **Design and implementation:** The degree of ease in obtaining consensus or overcoming obstacles to drive adoption of the solution
2. **Cost-benefit:** The degree to which the monetary investment is outweighed by gains in cybersecurity
3. **Applicability:** The degree to which the solution can be effectively tailored to different types of financial services institutions
4. **Pace of innovation:** The degree to which a solution minimizes obstacles to innovations in financial services

Solution 1: Cyber-risk metrics

The financial services industry currently struggles to effectively quantify cyber-risk. Compared to more mature disciplines like market and credit risk, approaches to estimate cyber-risk are less well-developed. This includes metrics for internal use, as well as external-facing metrics that are shared with regulators or with the public. Limited data also contributes to the challenge of accurately estimating the likelihood of a cyber-attack and the magnitude of an associated loss.

The impact of these limitations is that most cyber-risk metrics used today are not standardized, are difficult to understand and interpret, and fail to realize a core purpose: helping management and boards understand their cyber-risk exposure and loss potential in terms specific to their enterprise, their customers and the threat landscape.⁴

Advanced and standardized measures for cyber-risk quantification would help organizations to define their cyber-risk appetite and guide their cybersecurity investment decisions accordingly. Enhanced cyber-risk metrics would also support innovation by allowing firms to develop more accurate risk-based controls, including cyber-risk controls, for new technologies and processes.

Key benefits

- **Risk appetite definition:** Improved ability for companies to make an informed choice regarding the level of cyber-risk to customer data they are willing to accept, particularly for new innovations
- **Cybersecurity investment:** Enhanced capacity to calculate the return on cyber-risk investments
- **Comparability across industry:** Supports both companies and regulators in comparing cyber-risk across companies
- **Legacy system evaluation:** Ability to more accurately evaluate of the risk of legacy technology systems and determine whether they should be replaced
- **Cyber insurance:** Opportunity for insurers to expand cyber insurance market and to incentivize companies to invest in cybersecurity through risk-based policies

Next steps

A joint industry venture could develop a preliminary set of metrics. Where possible, this could leverage existing control frameworks, such as NIST.

Over time, enhanced metrics could also be used to support public-private collaboration, if regulators and companies can work together to agree on risk-based, rather than compliance-focused, metrics.

4. The challenges boards face in providing cyber-risk oversight are further described in a recent report by the World Economic Forum, “Advancing Cyber Resilience: Principles and Tools for Boards”.

Solution 2: Cybersecurity assessment

Given the proliferation of cybersecurity regulations and frameworks, it can be difficult for companies to evaluate and improve their cybersecurity readiness. This is most challenging for fintechs with constrained resources and pressure to quickly bring their offerings to market; however, it also affects incumbents who may wish to partner with them.

The development of cybersecurity guidance and assessment mechanisms for fintechs would help incumbents and challengers to better identify and adopt best practices. The proposed solution would include three parts: common principles for cybersecurity assessments and guidance for execution; a point-based scoring mechanism using the assessment criteria; and guidance on practical steps to improve an organization’s score.

Key benefits

- **Third-party risk evaluation:** Common understanding and comparable measurement of the risk faced by third-party providers and counterparties
- **Actionable solutions:** Clear and actionable mechanism for companies to improve cyber-posture (e.g. SWIFT Customer Security Program)
- **Increased cybersecurity standards:** De-risking of the broader system by raising standards across the board, including both technical and operational security
- **Enhanced innovation:** Focus on early-stage cybersecurity leading to more secure products that are more easily integrated into the broader financial services system
- **Cybersecurity by design:** Equal balance in commitment to cyber resilience and advancing the innovation frontier

Next steps

A small working group of public- and private-sector stakeholders could be convened, including incumbents, fintechs and technology companies.

This effort could be modelled on a similar project by the US Chamber of Commerce this summer on Critical Infrastructure Protection, Information Sharing and Cybersecurity. NIST is also in the process of updating its Framework for Improving Critical Infrastructure Cybersecurity.

Key stakeholders could develop a set of best practices that would meet regulatory guidance, and offer practical steps to increase security. It will also be important for the group to consider the scope of the assessment and how it will be operationalized.

Conclusion

Addressing cyber-risk – and implementing the solutions described in this whitepaper – will require cooperation both within and across the public and private sectors. The framework illustrated here can also be used to develop further solutions as technology and innovation continue to transform the nature of cyber-risk.

The private sector will need to balance business needs with the benefits of coordination. This can in part be achieved by the solutions that have been described in this document around common cyber-risk metrics and cybersecurity assessments. Incumbents and fintechs will also need to learn from each other, balancing innovation with the ability to scale while protecting against common threats.

Public sector actors will need to collectively work to balance cyber-risk management and the freedom to innovate. Regulators should focus on coordinating regulations across geographies and industries, and ensure that regulations incentivize risk management rather than compliance. Finally, the public and private sectors will need to come together to build trust within the system. By working together, financial services companies and regulators can also help to support the adoption and scale of industry solutions.

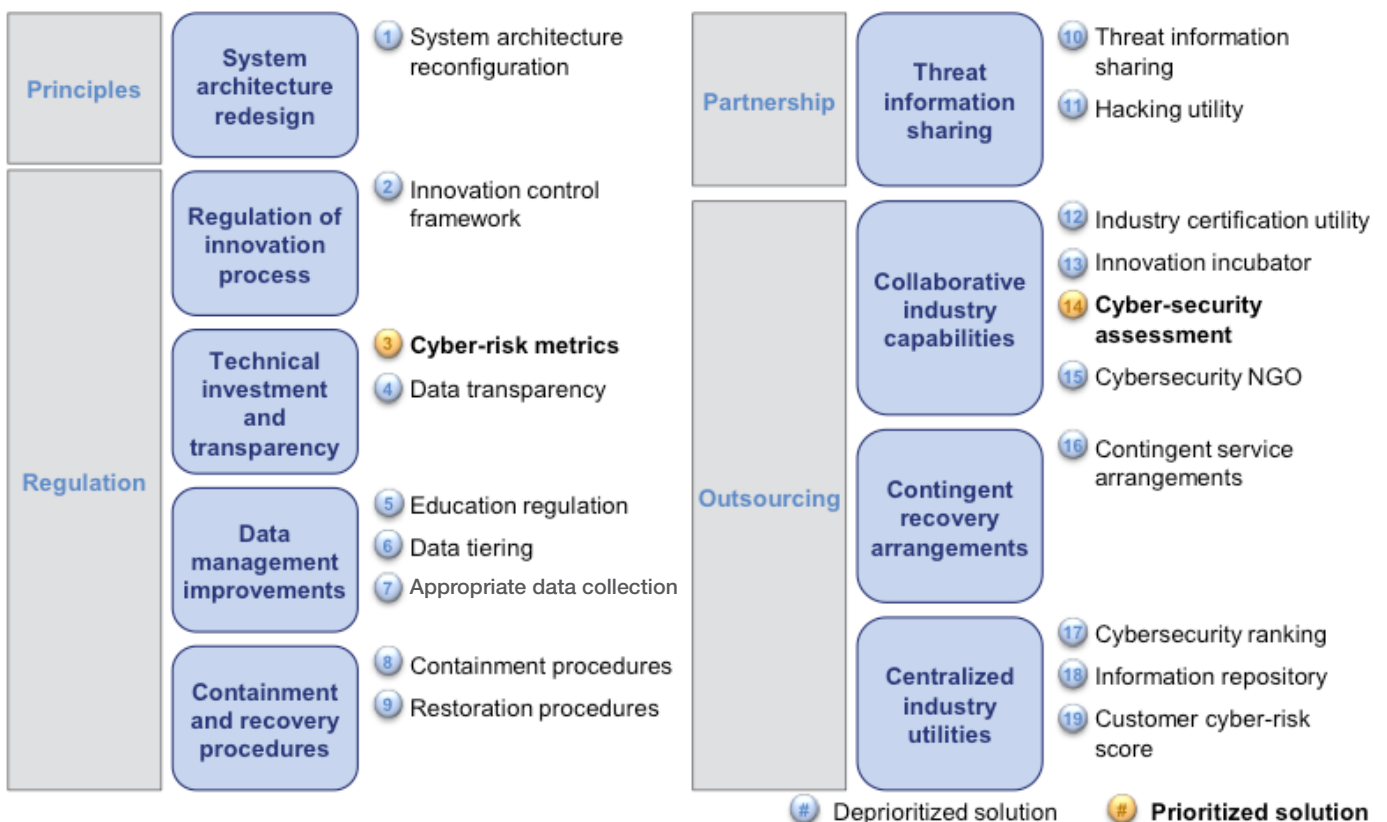
Appendix

Solution descriptions

The full list of 19 cyber-risk solutions is described below. Each solution includes a brief overview of the proposed initiative, the challenge it was developed to address, and key impact and feasibility considerations.

The solutions are grouped based on the nine solution categories identified in the document (e.g. cyber-risk lifecycle stage and implementations approach). They are strongly recommended for consideration by public- and private-sector actors across the financial services system.

Figure 6: Full list of solutions



Principles

System architecture design	<p>1. System architecture reconfiguration: Set of standards for embedding cyber-risk considerations when creating or restructuring IT systems</p> <ul style="list-style-type: none"> – Challenge: Financial Services institutions’ system architecture may not have been optimally designed to ensure the security of the data within the system – Impact: More secure technology through consideration of cybersecurity as part of business requirements, design and development process – Feasibility: High degree of design/implementation barriers with potential for large up-front cost
-----------------------------------	---

Regulation

Regulation of innovation process	<p>2. Innovation control framework: Framework to manage innovation-related cyber-risk as part of the product or service development process prior to launch in the market</p> <ul style="list-style-type: none"> – Challenge: There is significant pressure to innovate within financial services, which can cause institutions to deprioritize cybersecurity considerations when bringing new products to market – Impact: Increased focus on cybersecurity impact throughout the innovation process – Feasibility: Applicable to all financial services players; however, there is potential for design/implementation barriers
Technical investment and transparency	<p>3. Cyber-risk metrics: <i>See description on page 11</i></p>
	<p>4. Data transparency: Directive that requires informing customers what information is being collected and how it is being used, encouraging better data handling</p> <ul style="list-style-type: none"> – Challenge: Customers typically have limited insight into the information being collected about them or how it is being used by corporations. Many companies also have limited understanding of how customer data is being stored and processed throughout the organization. – Impact: More transparency around use of sensitive data, but no direct impact on attack likelihood or severity – Feasibility: Applicable to all financial services players, but potential for design/implementation barriers
Data management improvements	<p>5. Education regulation: Requirements for dedicated education programmes that encourage responsible data security practices by customers and employees</p> <ul style="list-style-type: none"> – Challenge: Employees and customers represent an attack surface for cyber-criminals and can expose institutions to harm if compromised – Impact: Increased awareness around data security and the implications of data sharing – Feasibility: No major design/implementation barriers; cost-benefit dependent on stringency of regulation
	<p>6. Data tiering: Data classification framework that differentiates protection requirements by level of sensitivity of the data</p> <ul style="list-style-type: none"> – Challenge: Many institutions, especially multinationals, struggle to determine which data should be classified as sensitive data and thus better protected – Impact: Improved data security practices through differentiation of data protection requirements – Feasibility: Difficulty to design standards applicable to all financial services players; cost-benefit dependent on stringency of regulation
	<p>7. Appropriate data collection: Standards limiting data collection scope for financial services firms, ensuring that only necessary financial information is collected</p> <ul style="list-style-type: none"> – Challenge: Due to regulatory and business pressures, financial services institutions collect as much data on customers as possible, even though it might not all be required to provide services to customers – Impact: Reduced “attractiveness” of financial services data to cyber-attackers – Feasibility: High degree of design/implementation barriers

Containment and recovery procedure	<p>8. Containment procedures: Procedures outlining actions to be taken upon diagnosis of a data breach</p> <ul style="list-style-type: none"> – Challenge: Institutions may not have clear action plans or “playbooks” to prevent further spread of a cyber-attack once systems have been compromised – Impact: Reduced cyber-attack severity, especially for less sophisticated players – Feasibility: No major design/implementation barriers; difficult to design procedures that are applicable to all financial services players
	<p>9. Restoration procedures: Procedures outlining recovery actions to be taken after a data breach has been arrested</p> <ul style="list-style-type: none"> – Challenge: Institutions may not have clear action plans or “playbooks” to ensure timely restoration of systems once a breach occurs – Impact: Faster recovery time post-cyber-attack, especially for less sophisticated players – Feasibility: No major design/implementation barriers; difficult to design procedures that are applicable to all financial services players

Partnership

Threat information sharing	<p>10. Threat information sharing: Centralized platform with shared industry resources commissioned to provide threat identification services</p> <ul style="list-style-type: none"> – Challenge addressed: Competitive and business pressures prevent financial services players from collaborating effectively – Impact: Faster identification of potential cyber-threats and development of solutions – Feasibility: Applicable to all financial services players; difficult to define cross-border access/participation requirements; need for coordination between existing information sharing efforts; liability considerations
	<p>11. Hacking utility: Regulation ensuring that technical debt is addressed through incentive schemes and/or industry requirements</p> <ul style="list-style-type: none"> – Challenge: Companies are often not aware of weaknesses in their security systems, leaving them open for attack, and information on vulnerabilities may not be shared widely or rapidly enough – Impact: Faster identification of new cybersecurity vulnerabilities through coordinated efforts – Feasibility: Applicable to all financial services players; strict oversight and governance processes would be required for results sharing

Collaborative industry capabilities	<p>12. Industry certification utility: Industry utility that offers a certification of companies that provide cybersecurity services to the financial services industry</p> <ul style="list-style-type: none"> – Challenge: With the proliferation of cybersecurity firms, many financial services institutions struggle to identify the highest-quality offerings for these critical services – Impact: Transparent and independent quality assessment of cybersecurity services – Feasibility: Applicable to all financial services players; effect on innovation dependent on stringency of certification requirements
	<p>13. Innovation incubator: A centralized incubator, backed by financial services institutions, which promotes/supports start-ups innovating in the cybersecurity space</p> <ul style="list-style-type: none"> – Challenge: Cyber-attackers are innovating very rapidly and it is difficult for institutions to innovate as quickly on cybersecurity – Impact: Increased pace of cybersecurity innovation and increased return on cybersecurity investments (i.e. minimizes duplicative efforts) – Feasibility: No major design/implementation barriers
	<p>14. Cybersecurity assessment: <i>See description on page 11</i></p>
	<p>15. Cybersecurity NGO: Centralized non-profit entity, overseen by incumbents, to provide cybersecurity services for early-stage fintechs</p> <ul style="list-style-type: none"> – Challenge: New market entrants often do not have the resources or expertise to practice effective cybersecurity and can represent the “weakest link” in the financial services system – Impact: Faster access to innovative products, services and technologies that incorporate cybersecurity considerations as part of the design – Feasibility: No major design/implementation barriers
Contingent recovery arrangements	<p>16. Contingent service arrangements: Capabilities that allow financial institutions to provide services for their competitor’s customers in the event of an attack</p> <ul style="list-style-type: none"> – Challenge: Financial institutions offer critical services to customers and may be unable to do so in the event of a severe cyber-attack – Impact: Increased operational stability during cyber-attacks, reducing monetary losses – Feasibility: Applicable to all financial services players; design/implementation barriers dependent on the scope of the arrangement and associated liabilities
Centralized industry utilities	<p>17. Cybersecurity ranking: Independent entity that collects cybersecurity information and provides institutions with a cybersecurity ranking against its competitors</p> <ul style="list-style-type: none"> – Challenge: Financial services industry players are not aware of how their cyber-resilience stacks up against their competitors – Impact: Consistent assessment and benchmarking of preparedness for cyber-attacks incentivizes higher level of cybersecurity across the financial services industry – Feasibility: High barrier to information sharing; risk of adverse effects (e.g. target of the weakest, bank run) if information is leaked to the public domain
	<p>18. Information repository: Central, cross-industry repository and guardian of sensitive customer data that provides access as a service to financial institutions</p> <ul style="list-style-type: none"> – Challenge: Businesses collect and house large amounts of customer data, increasing concentration risk and attractiveness to attackers – Impact: Reduced “attractiveness” of financial services data to cyber-attackers – Feasibility: Potential resistance due to loss of customer data ownership; high degree of design and implementation difficulties; risk that repository could become a target for hackers
	<p>19. Customer cyber-risk score: A central utility that collects information about customers to assess customer cyber-risk, assigning a score similar to a credit score</p> <ul style="list-style-type: none"> – Challenge: Customers represent an attack surface for cyber-criminals, both to perpetuate fraud (which can be costly) and carry out more damaging cyber-attacks – Impact: Increased awareness around data security and the implications of data sharing and ability of financial institutions to target cybersecurity efforts – Feasibility: Applicable to all financial services players; potential negative impact on access to financial services

References

- Accenture, *The State of Cybersecurity and Digital Trust 2016: Identifying Cybersecurity Gaps to Rethink State of the Art*, 2016.
- Australian Securities & Investments Commission, *Cyber resilience: Health check*, 2015.
- Cisco, *Cisco Global Cloud Index: Forecast and Methodology, 2016–2021*, 2017.
- Deloitte, *Transforming cybersecurity: New approaches for an evolving threat landscape*, 2014.
- Financial Stability Institute, *Regulatory approaches to enhance banks' cybersecurity frameworks*, 2017.
- Georgia Tech Information Security Center, *Governance of Cybersecurity: 2015 Report*, 2015.
- Grace, Andrew, *Managing cyber-risk – the global banking perspective*, 10 June 2014, speech presented at BBA, London.
- Harvard Business Review, *Why is Cybersecurity So Hard*, May 2017.
- Mandiant, *M-Trends 2017: A View From the Front Lines*, 2017.
- Marsh, Global Risks, *European 2015 Cyber Risk Survey Report*, 2015.
- Marsh & McLennan, *MMC Cyber Handbook 2018: Perspectives on the next wave of cyber*, 2017.
- Massachusetts Institute of Technology, *How companies achieve balance between technology enabled innovation and cyber-security*, 2016.
- Oliver Wyman, *Cyber Risk in Asia Pacific: The Case for Greater Transparency*, 2017.
- Oliver Wyman, *Deploying a Cyber Risk Strategy: Five Key Moves Beyond Regulatory Compliance*, 2017.
- Oliver Wyman, *Embedding Cyber Defenses Where They Matter*, 2017.
- Oliver Wyman, *The Equifax Data Breach: And its impact on identity verification*, 2017.
- The Financial Services Roundtable – BITS, *Cybersecurity Regulatory Harmonization*, 2017.
- The President's National Infrastructure Advisory Council (NIAC), *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*, 2017.
- Tuveson, Michelle, "Why the world should pay attention to cyber risks", *Forum Blog*, 19 January, 2016.
- World Economic Forum, *Advancing Cyber Resilience: Principles and Tools for Boards*, 2017.
- World Economic Forum, *Global Agenda Council on Cybersecurity*, 2016.
- World Economic Forum, *Recommendations for Public – Private Partnership against Cybercrime*, 2016.
- World Economic Forum, *Realizing the Potential of Blockchain*, 2017.
- World Economic Forum, *Understanding Systemic Cyber Risk*, 2016.
- World Economic Forum in collaboration with Oliver Wyman, *The Role of Financial Services in Society: Understanding the impact of technology-enabled innovation on financial stability*, 2016.

Acknowledgements

Stewards of the System Initiative on Shaping the Future of Financial and Monetary Systems

The project team offers its special gratitude to the members of the System Initiative on Shaping the Future of Financial and Monetary Systems for their oversight of the Balancing Financial Stability, Innovation and Economic Growth initiative.

Stewards

Oliver Bäte, Chief Executive Officer, Allianz, Germany

Eric Jing, Chief Executive Officer, Ant Financial Services Group, People's Republic of China

Ana Botín, Group Executive Chairman, Banco Santander, Spain

Brian T. Moynihan, Chairman of the Board and Chief Executive Officer, Bank of America Corporation, USA

Stephen S. Poloz, Governor of the Bank of Canada

Mark Carney, Governor of the Bank of England

Haruhiko Kuroda, Governor of the Bank of Japan

Laurence D. Fink, Chairman and Chief Executive Officer, BlackRock, USA

Patrick Njoroge, Governor of the Central Bank of Kenya

Elvira Nabiullina, Governor of the Central Bank of the Russian Federation

Mauricio Cardenas, Minister of Finance and Public Credit of Colombia

Tidjane Thiam, Chief Executive Officer, Credit Suisse, Switzerland

Michael C. Bodson, President and Chief Executive Officer, Depository Trust & Clearing Corporation (DTCC), USA

John Cryan, Chief Executive Officer, Deutsche Bank, Germany

Jeroen Dijsselbloem, President, Euro Group

David Lipton, First Deputy Managing Director, International Monetary Fund (IMF), Washington DC

Ralph Hamers, Chief Executive Officer, ING Group, Netherlands

Pier Carlo Padoan, Minister of Economy and Finance of Italy

Roberto Egydio Setubal, President and Chief Executive Officer, Itaú Unibanco, Brazil

Daniel Glaser, President and Chief Executive Officer, Marsh & McLennan Companies (MMC), USA

Ajay S. Banga, President and Chief Executive Officer, Mastercard, USA

José Antonio Meade Kuribreña, Minister of Finance of Mexico

John Rwangombwa, Governor of the National Bank of Rwanda (NBR)

Min Zhu, Chairman, National Institute of Financial Research, People's Republic of China

Dan Schulman, Chief Executive Officer, PayPal, USA

José Viñals, Chairman, Standard Chartered Bank, United Kingdom

Axel A. Weber, Chairman of the Board of Directors, UBS, Switzerland

H.M. Queen Máxima of the Netherlands; United Nations Secretary-General's Special Advocate for Inclusive Finance

Alfred F. Kelly Jr, Chief Executive Officer, Visa, USA

Joaquim Levy, Managing Director and Chief Financial Officer, World Bank Group, Washington DC

Tom de Swaan, Chairman of the Board, Zurich Insurance Group, Switzerland

Steering Committee

The project team thanks the members of the multistakeholder Steering Committee for their leadership of the Balancing Financial Stability, Innovation and Economic Growth initiative.

Members

Stefano Aversa, Global Vice-Chairman and Chairman EMEA, AlixPartners, United Kingdom
Greg Medcraft, Chairman, Australian Securities and Investment Commission (ASIC), 2011-2017
Khalid Al Rumaihi, Chief Executive, Bahrain Economic Development Board, Bahrain
Sanjiv Bajaj, Managing Director, Bajaj Finserv, India
Thong Nguyen, President, Retail Banking; Co-Head, Consumer Banking, Bank of America Corporation, USA
Stephen S. Poloz, Governor of the Bank of Canada
Hedva Ber, The Supervisor of Banks, Bank of Israel, Israel
Jes Staley, Chief Executive Officer, Barclays, United Kingdom
Barbara Novick, Vice-Chairman, BlackRock, USA
Bertrand Badré, Chief Executive Officer, BlueOrange Capital, USA
Kevin Lynch, Vice-Chairman, BMO Financial Group, Canada
Cecilia Skingsley, Deputy Governor of the Central Bank of Sweden (Sveriges Riksbank)
Elvira Nabiullina, Governor of the Central Bank of the Russian Federation
Michael C. Bodson, President and Chief Executive Officer, Depository Trust & Clearing Corporation (DTCC), USA
Tom Woolf, Founder and Chief Executive Officer, EdAid, United Kingdom
Adam Farkas, Executive Director, European Banking Authority, United Kingdom
Benoît Coeuré, Member of the Executive Board, European Central Bank, Frankfurt
Maria Clemencia Sierra, Chief Financial Officer, FDN (Financiera de Desarrollo Nacional), Colombia
Clemente del Valle, President, FDN (Financiera de Desarrollo Nacional), Colombia
Domingo Sugranyes Bickel, Chairman, Fondazione Centesimus Annus Pro Pontifice, Vatican City State
Nauman K. Dar, President and Chief Executive Officer, Habib Bank, Pakistan
Ralph Hamers, Chief Executive Officer, ING Group, Netherland
Erik Berglöf, Professor and Director, Institute for Global Affairs, London School of Economics, United Kingdom
Matthew Gamser, Chief Executive Officer, Small and Medium Enterprise Finance Forum, International Finance Corporation (IFC), Washington DC
Paul Andrews, Secretary-General, International Organization of Securities Commissions (IOSCO), Spain
Fabrizio Pagani, Head of the Technical Secretariat, Office of the Ministry of Economy and Finance of Italy
Richard Eldridge, Chief Executive Officer, Lenddo, Singapore
Jeff Stewart, Founder and Chairman, Lenddo, Singapore
Juan Colombas, Chief Risk Officer and Member of the Board of Directors, Lloyds Banking Group, United Kingdom
Kush Saxena, Executive Vice-President, Strategy and Corporate Development, Mastercard, USA
Domenico Giovanni Siniscalco, Vice-Chairman; Country Head, Italy, Morgan Stanley, Italy
Alain Demarolle, Chairman, My Money Bank, France
Greg Medcraft, Director, Organization for Economic Co-operation and Development (OECD), Paris
Franz Paasche, Senior Vice President, Corporate Affairs and Communications, PayPal, USA
David McKay, President and Chief Executive Officer, RBC (Royal Bank of Canada), Canada
Mark Hawkins, President and Chief Financial Officer, Salesforce, USA
Jeff Lynn, Chief Executive Officer, Seedrs, United Kingdom
Eric Parrado, Superintendent of Banks and Financial Institutions of Chile
Thomas Moser, Alternate Member of the Governing Board, Swiss National Bank, Switzerland
Hikmet Ersek, President and Chief Executive Officer, The Western Union Company, USA
Michael Budolfson, President, UNI Europe Finance, UNI Global Union, Switzerland
Randall Kroszner, Norman R. Bobins Professor of Economics, University of Chicago, USA
Ellen Richey, Vice-Chairman, Risk and Public Policy, Visa, USA
Kapil Wadhawan, Chairman, Wadhawan Group, India
Brian Hartzler, Chief Executive Officer and Managing Director, Westpac Banking Corporation, Australia
Cahit Erdogan, Assistant General Manager, Yapi Kredi Bank, Turkey
Giles Andrews, Co-Founder and Chief Executive Officer, Zopa, United Kingdom

Cyber Working Group

The project team also thanks the Cyber Working Group for its contributions to the Balancing Financial Stability, Innovation and Economic Growth initiative.

Members

Jon Rigby, Director Cyber, Intelligence and Information Integration, AlixPartners, United Kingdom
Gretchen Ruck, Head of Cyber-Security, AlixPartners, USA
WuJie Yu, Chief Data Scientist, Ant Financial Services Group, People's Republic of China
Tao Sun, Senior Economist, Ant Financial Services Group, People's Republic of China
Oliver Harvey, Senior Executive Leader, Market Infrastructure, Australian Securities and Investment Commission (ASIC), Australia
Rakesh Bhatt, Chief Operation Officer, Baja Finance, Baja Finserve, India
Craig Froelich, Chief Information Security Officer, Bank of America Corporation, USA
Filipe Dinis, Chief Operating Officer, Bank of Canada, Canada
Fred Reinthaler, Security Solutions Integrator, Bank of Canada, Canada
Kfir Godrich, Chief Technology Officer, BlackRock, USA
Michael Cooper, Chief Technology Officer, Global Banking and Financial Markets, BT Group, United Kingdom
Anton Tolstikov, Senior Adviser to the Executive Director for the Russian Federation in the IMF, Central Bank of the Russian Federation, Russian Federation
Jason Harrell, Head of TRM Risk Analysis and Reporting, Depository Trust & Clearing Corporation (DTCC), USA
Frank Fischer, Chief Information Security Officer, Deutsche Börse, Germany
Evgueni Ivantsov, Chairman, European Risk Management Council, United Kingdom
Nida Davis, Associate Director, Division of Supervision and Regulation, Federal Reserve System, USA
Tim Maas, Assistant Director, Division of Reserve Bank Operations and Payment Systems, Federal Reserve System, USA
Tony Cole, Vice-President, Global Government CTO, FireEye, USA
Lucy Vernall, General Global Counsel and Head of Compliance, Funding Circle, United Kingdom
Nat Mokry, Senior Director, Cyber Security, Hewlett Packard Enterprise, USA
Deborah Eng, Executive Director in the Global Cyber Partnerships & Government Strategy, JP Morgan Chase & Co., USA
Clint Hill, Head of Architecture and Platform Solutions, Kabbage, USA
Anton Shingarev, Vice-President, Public Affairs, Kaspersky Lab, Russian Federation
Paul Vlssidis, Technical Director - Senior Advisor, NCC Group, United Kingdom
Mason Rice, Oak Ridge National Laboratory, USA
David Fairman, Chief Information Security Officer, RBC (Royal Bank of Canada), Canada
James Alkove, Executive Vice-President for Security, Salesforce.com, USA
Aleksandr Yampolskiy, Co-Founder and Chief Executive Officer, Security Scorecard, USA
Jasson Casey, Chief Technology Officer, Security Scorecard, USA
Ricardo Brizido, Chief Technology Officer, Seedrs, United Kingdom
Cheri McGuire, Chief Information Security Officer, Standard Chartered Bank, United Kingdom
Richard Nash, Head, Global Government Relations, PayPal, USA
Mike Kalac, Chief Information Security Officer, The Western Union Company, USA
Mark Etherington, Global ETI Technology, Thomson Reuters, USA
Shan Lee, Information Security Officer, TransferWise, United Kingdom
Steve Weber, Professor of Political Science & I-School, UC Berkeley, USA
David Symington, Policy Specialist at the Office of the Secretary General's Special Advocate for Inclusive Finance (UNSGSA) , United Nations, New York
Michael Nunes, Senior Director, Innovation & Technology Policy, Visa, USA
Rich Baich, Chief Information Security Officer, Wells Fargo, USA
Ross MacKenzie, Head of Security Governance, Information Security Group, Westpac Banking Corporation, Australia
Aquiles Almansi, Lead Financial Sector Specialist, World Bank, Washington DC
Yener Kilic, Cybersecurity Head, Yapi Kredi Bank, Turkey
Brent Phillips, Chief Information Security Officer, Zurich Insurance Group, Switzerland

Project Team

The development of this White Paper was supported by the project team:

Members

Matthew Blake, Head of the Future of Financial and Monetary Systems Initiative, World Economic Forum

Kai Keller, Project Lead, Balancing Financial Stability, Innovation, and Economic Growth Initiative, World Economic Forum

Ted Moynihan, Managing Partner and Global Head, Financial Services, Oliver Wyman (MMC), United Kingdom

Douglas Elliott, Partner, Financial Services, Oliver Wyman (MMC), USA

Paul Mee, Partner, Financial Services, Oliver Wyman (MMC), USA

Rico Brandenburg, Principal, Financial Services, Oliver Wyman (MMC), USA

Matthew Gruber, Associate, Financial Services, Oliver Wyman (MMC), USA

Alison Flint, Associate, Financial Services, Oliver Wyman (MMC), USA



**COMMITTED TO
IMPROVING THE STATE
OF THE WORLD**

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org