BIS

BIS Bulletin

No 37

Covid-19 and cyber risk in the financial sector

Iñaki Aldasoro, Jon Frost, Leonardo Gambacorta and David Whyte

14 January 2021

BIS Bulletins are written by staff members of the Bank for International Settlements, and from time to time by other economists, and are published by the Bank. The papers are on subjects of topical interest and are technical in character. The views expressed in them are those of their authors and not necessarily the views of the BIS. The authors are grateful to Giulio Cornelli for excellent analysis and research assistance, and to Louisa Wagner for administrative support.

The editor of the BIS Bulletin series is Hyun Song Shin.

This publication is available on the BIS website (www.bis.org).

ISSN: 2708-0420 (online)
ISBN: 978-92-9197-451-0 (online)

Iñaki Aldasoro
inaki.aldasoro@bis.org

Jon Frost
jon.frost@bis.org

Leonardo Gambacorta
leonardo.gambacorta@bis.org

David Whyte
david.whyte@bis.org

Covid-19 and cyber risk in the financial sector

Key takeaways

- *The financial sector has been hit by hackers relatively more often than other sectors during the Covid-19 pandemic.*
- *While this has not yet led to significant disruptions or a systemic impact, there are substantial risks from cyber attacks for financial institutions, their staff and their customers going forward.*
- *Financial authorities are working to mitigate cyber risks, including through international cooperation.*

During the Covid-19 pandemic, financial institutions have been at the leading edge of the response to cyber risk. Their already large exposure to cyber risk has been further accentuated by the move towards more working from home (WFH) and other operational challenges. This Bulletin serves as a primer on cyber risk and presents initial findings on how the financial sector has met the challenges of the pandemic. We draw on new data to assess changes in the threat landscape for financial institutions in the pandemic.

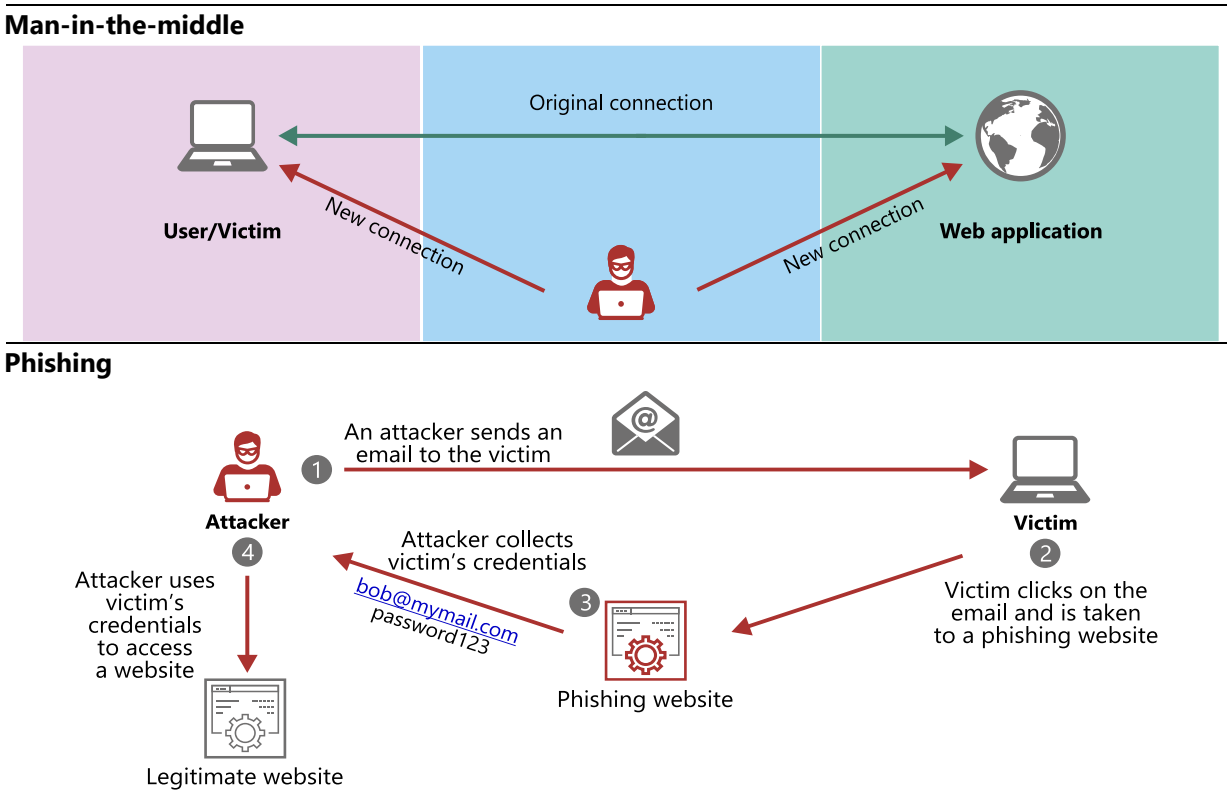
Cyber risk: a taxonomy

As the economy and financial system become more digitised, cyber risk is growing in importance. "Cyber risk" is an umbrella term encompassing a wide range of risks resulting from the failure or breach of IT systems. According to the FSB Cyber Lexicon (2019), cyber risk refers to "the combination of the probability of cyber incidents occurring and their impact". A "cyber incident", in turn, is "any observable occurrence in an information system that: (i) jeopardises the cyber security of an information system or the information the system processes, stores or transmits; or (ii) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not". Cyber risk is one form of operational risk (Aldasoro et al (2020b), CPMI-IOSCO (2016)). Cyber risks can be classified based on their cause/method, actor, intent and consequence (Aldasoro et al (2020a), Curti et al (2019)).

The causes or methods vary, and include both unintended incidents and intentional attacks. Examples of the former are accidental data disclosure, and implementation, configuration and processing errors. Such incidents are frequent. Yet around 40% of cyber incidents are intentional and malicious, rather than accidental, ie they are cyber attacks (Aldasoro et al (2020c)).

Some cyber attacks involve threat actors inserting themselves into a trusted data exchange. *Malware* (ie "malicious software") is software designed to cause damage to IT devices and/or steal data (for example, so-called Trojans, spyware and ransomware). *Man-in-the-middle attacks* occur when attackers insert themselves into a two-party transaction (Graph 1, first panel), accessing or manipulating data or transactions. *Cross-site scripting* is a web security vulnerability that allows attackers to compromise the interactions a victim has with a vulnerable application. *Phishing* is stealing sensitive data or installing malware with fraudulent emails that appear to be from a trustworthy source (Graph 1, second panel). To gain a victim's trust, phishing attacks may imitate trusted senders. After gaining entrance, these may help attackers to gain credentials and entry into a system. *Password cracking* is the process of recovering secret passwords stored in a computer system or transmitted over a network.

Selected causes of cyber attacks Graph 1



Source: Authors' elaboration.

Some attacks involve professional tools and planning. *A zero-day exploit* is an attack against a software or hardware vulnerability that has been discovered but not publicly disclosed (Graph 1, third panel). The discovery of a zero-day exploit can result in a situation where both the customers and vendors

of the IT asset are now subject to cyber attacks for which no predefined detection signatures or remedial patches are available. Exacerbating this situation are commercial firms that conduct research to sell zero-day exploits on the open market. Some of these firms, such as Zerodium, pay large cash rewards (up to $2.5 million) for high-risk vulnerabilities. Finally, *distributed denial of service (DDoS) attacks* flood servers with traffic to exhaust bandwidth or consume finite resources (Graph 1, fourth panel). These attacks may require renting computing capacity, or hacking third-party devices, to participate in an attack.

Actors include outright criminal and terrorist organisations, industrial spies, "hacktivists", or state and state-sponsored players. The damage they can cause depends on their sophistication and resources. For example, in 2016, hackers associated with North Korea carried out a notable attack by breaching the systems of Bangladesh Bank and using the SWIFT network to send fraudulent money transfer orders (Bangladesh Bank-FRBNY (2019)). The attack highlighted rising cyber risks for payment systems and associated infrastructures.[1] The ultimate purpose can be for profit (eg ransomware, industrial spying), geopolitical (state-sponsored attacks on critical infrastructures) or general discontent (hacktivism).

The consequences of cyber attacks can be severe. Business disruptions and IT system failures can damage the integrity and availability of assets and services. Data breaches compromise the confidentiality of sensitive data, with financial and reputational losses. Fraud and theft include the loss of funds or any information (eg intellectual property) that may or may not be personally identifiable. In some circumstances, cyber attacks could have systemic implications and cause serious economic dislocations.

Covid-19, remote working and changes in the cyber threat landscape

Covid-19 has precipitated a move to working from home (WFH). Financial institutions – like other organisations – have temporarily shifted to remote working to protect their workers. Moving the majority of activities to the digital world could increase the risk of cyber attacks. For instance, the use of remote access technologies such as the remote desktop protocol (RDP) and virtual private network (VPN) increased by 41% and 33%, respectively, in the first two months of the Covid-19 outbreak (ZDNet (2020)). Unless well managed, this may allow new opportunities for threat actors to penetrate IT systems and carry out cyber attacks, along with other types of financial crime (Crisanto and Prenio (2020)). WFH may also challenge business continuity plans and the response to an operational or cyber incident.

The recent SolarWinds hack underscores risks from third-party vendors. In December 2020, it was reported that hackers had inserted malware into the company SolarWinds' product Orion, used by thousands of companies and government agencies around the world (FBI-CISA-ODNI (2020)). Software supply chain attacks are one of the hardest types of threat to mitigate, as they take advantage of established trust relationships and the machine-to-machine communications used to provide essential software updates. While the financial sector was not a primary target, the hackers gained access in March 2020 and remained undetected for many months. The full scale of the attack has not been fully disclosed.[2]

The financial sector has been hit relatively more often by cyber attacks than most other sectors since the pandemic started. Data on attacks can be obtained from Advisen, a for-profit organisation that collects information from reliable and publicly verifiable sources (mostly in the United States), covering date, actor, loss amount and other features. There is a strong link between the prevalence of WFH arrangements – as measured by the WFH index by sector from Dingel and Neiman (2020) – and the incidence of cyber attacks between the end of February and June 2020 (Graph 2, left-hand panel). The financial sector ranks high on both accounts (red square). Outside the health sector, the financial sector has the largest share of cyber events classified as Covid-19-related in recent months (right-hand panel). Examples are phishing attacks that explicitly use the uncertainty around Covid-19 to entice users to open fraudulent attachments or grant attackers access to networks.

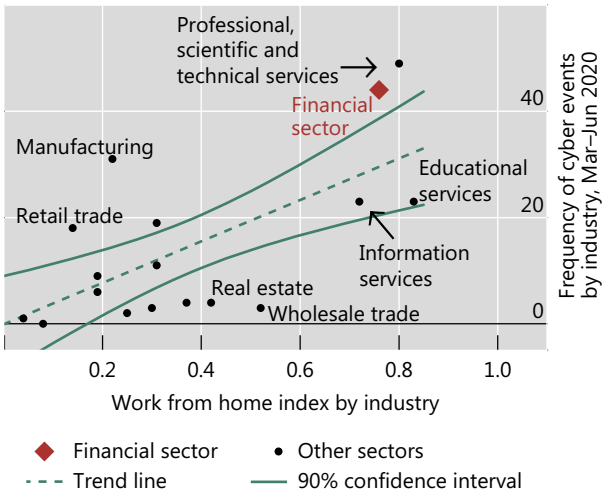
[1] In response to ever more sophisticated attacks, SWIFT launched a Customer Security Programme (CSP) in 2016 (SWIFT (2019)).

[2] Separately, in January 2021, the Reserve Bank of New Zealand (RBNZ) reported that a third-party file sharing service that the Bank used to share and store some sensitive information was illegally accessed (RBNZ (2021)).

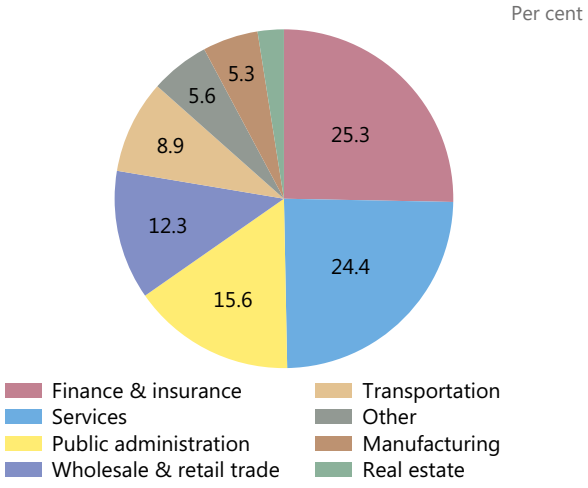
Payment firms, insurers and credit unions have been especially affected. A survey among financial institutions by the Financial Services Information Sharing and Analysis Center (FS-ISAC) finds a substantial rise in phishing, suspicious scanning and malicious activity against webpages for WFH staff to access the network. Payment firms, insurance companies and credit unions have seen the strongest increase in hacks (Graph 3, left-hand panel). Covid-19-related attacks grew with the spread of the pandemic, from fewer than 5,000 per week in February to more than 200,000 per week in late April. They rose further by around one third in May and June compared with March and April (Check Point Research (2020)). The survey highlighted that, in 45% of cases, staff WFH overwhelmed virtual desktop infrastructure (VDI)/VPN processes. In one third of cases, business continuity IT plans were not prepared for a long-term at-home work force (right-hand panel). One fifth of the financial firms reported that their network operation activities were interrupted during the pandemic.

The financial sector has been hit by cyber attacks during the pandemic — Graph 2

WFH index versus cyber events during Covid-19[1]



Covid-19-related cyber events by sector[2]



[1] Excludes the health sector. [2] Based on cases classified by Advisen as Covid-19-related. Includes data up to 9 September 2020. The sample in the graph excludes the health sector (57 Covid-related cases) and affecting health-related items of the manufacturing sector (163 cases).

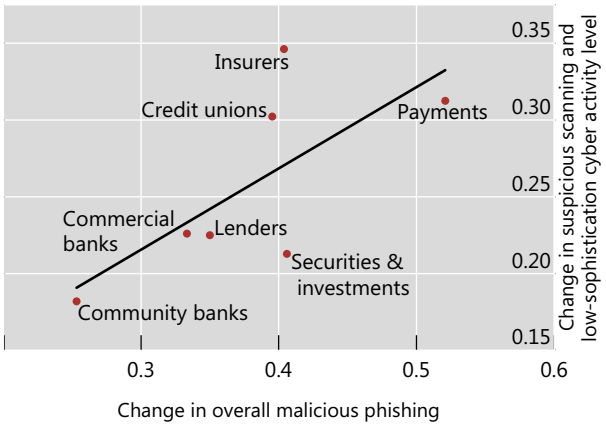
Sources: Dingel and Neiman (2020); Advisen; authors' calculations.

Mass migration to WFH can make financial institutions' staff more vulnerable. As staff work from home through firm-issued and private devices and networks, new risks may arise. In a household, multiple family members could be logging on to the same network, potentially exposing devices to malware that could then enter a firm's enterprise environment. Some videoconferencing facilities have been shown to have suboptimal security standards. Trader surveillance may also be subject to unintended consequences. Regulatory rules require that traders' calls are recorded and monitored, but traders have been working from home and calls may go unrecorded. Another factor at play is the expansion of the range of self-service options available to customers online – for wealth management trades, mortgage, loan applications, etc. Ensuring robust security controls becomes even more essential.

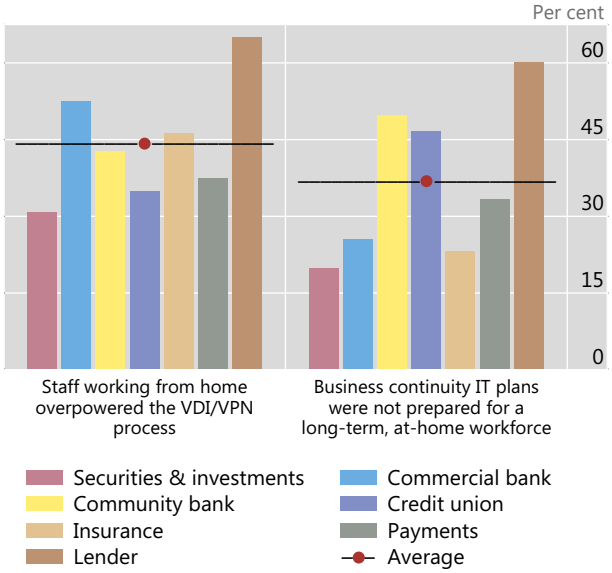
Evidence so far suggests the same threat actors, intent and methods as before the pandemic, but new opportunities given Covid-19-related uncertainty. Phishing ploys are not new, but the volume of such attempts has spiked. A recent report found that a quarter of cyber incidents responded to in the United Kingdom over August 2019–August 2020 involved criminals and hostile states exploiting the Covid-19 pandemic (NCSC (2020)). In the European Union (EU), threat actors compromised the VPN services of EU institutions that allow staff to work from home (CERT-EU (2020)). In other cases, threat actors imitated trusted sources such as the World Health Organization to get users to open malicious links and files (Microsoft (2020)). In one case, a DDoS attack was able to disrupt trading at a major stock exchange for four consecutive days (Hope (2020)), underscoring the risks of hacking to critical infrastructures.

Working from home (WFH) opens up new possibilities for cyber attacks[1] Graph 3

Cyber attacks increased during the Covid-19 period, with differences across financial firm types[2]



WFH overpowers VDI/VPN processes and business continuity plans[3]



[1] The graphs report the results of a survey by FS-ISAC among financial institutions in April 2020. [2] The first question (results reported on the horizontal axis) is: "During the past few months, has your firm experienced a change in overall malicious phishing levels?". The second question (results reported on the vertical axis) is: "During the past few months, has your firm experienced a change in overall suspicious scanning or other low-sophistication cyber activity levels?". The results of the survey are summarised by a Covid-19 cyber attack diffusion index, which aggregates answers. Financial institutions that answered "considerably" are given a weight of 1; those that answered "somewhat" receive a score of 0.5. The index ranges between –1 and 1. A positive value indicates an increase in cyber attacks. [3] The first question (results reported on the left) is: "Did staff working from home overpower your VDI/VPN process?". The second question (results reported on the right) is: "Were business continuity IT plans prepared for a long-term, at-home workforce?". The panel gives the share of firms that answered "yes".

Source: FS-ISAC (2020).

Policies to reduce risks to financial stability

Policy must take account of two near-term trends. First, remote work is likely to remain higher than in the pre-Covid-19 period. Business continuity plans designed for short-term disruptions may need to adapt to WFH over longer periods, and business processes may need to adapt to the "new normal". Second, financial institutions are likely to continue to move parts of their IT operations to public cloud environments. As the market for cloud services is highly concentrated, there are warnings about increased homogeneity in the financial sector and single points of failure (Danielson and Macrae (2019)). A recent survey indicates that 82% of companies increased cloud usage as a result of the coronavirus pandemic and 91% are planning a more strategic use of cloud in the near future (Snow (2020)). Through shared software, hardware and vendors, incidents could, in principle, spread more quickly, leading to higher losses for financial institutions and stress in the financial system (Welburn and Strong (2019)).

Policymakers and businesses are actively working together to mitigate cyber risks and their systemic implications. For instance, many private and public sector organisations are strengthening their operational resilience, and many have engaged in "war games" or simulations of cyber attacks. These exercises can help to identify vulnerabilities and enhance preparedness and line of communication. Moreover, financial supervisors and overseers are leveraging national or international standards or guidance to promote cyber resilience.[3] In addition to global initiatives, there are several regional groups and cooperation forums. The BIS will continue supporting international cooperation in this area, recognising that cyber resilience is fundamentally a global public good (Cœuré (2019), Carstens (2019)).

[3] For relevant standards and practices, see CPMI-IOSCO (2016), IAIS (2016), FSB (2017) and BCBS (2018) among others.

References

Aldasoro, I, J Frost, L Gambacorta, T Leach and D Whyte (2020a): "Cyber risk in the financial sector", SUERF Policy Notes, no 206, November.

Aldasoro, I, L Gambacorta, P Giudici and T Leach (2020b): "Operational and cyber risks in the financial sector", BIS Working Papers, no 840, February.

--- (2020c): "The drivers of cyber risk", BIS Working Papers, no 865, May.

Bangladesh Bank and Federal Reserve Bank of New York (FRBNY) (2019): "Joint Statement", 1 February.

Basel Committee on Banking Supervision (BCBS) (2018): Cyber-resilience: range of practices, December.

Carstens, A (2019), "The new BIS strategy – bringing the Americas and Basel closer together", speech, Lima, 1 October.

Check Point Research (2020): Cyber attack trends: 2020 mid-year report, July.

Cœuré, B (2019): "Cyber resilience as a global public good", speech, Paris, 10 May.

Committee on Payments and Market Infrastructures and International Organization of Securities Commissions (CPMI-IOSCO) (2016): Guidance on cyber resilience for financial market infrastructures, June.

Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU) (2020): "Direct threats to EU institutions, bodies and agencies", 19 October.

Crisanto, J and J Prenio (2020): "Financial crime in times of Covid-19 – AML and cyber resilience measures", FSI Brief, no 7, May.

Curti, F, J Gerlach, S Kazinnik, M Lee and A Mihov (2019): "Cyber risk definition and classification for financial risk management", Federal Reserve Bank of St Louis, August, mimeo.

Dingel, J and B Neiman (2020): "How many jobs can be done at home?", Journal of Public Economics, 189, September.

Financial Services Information Sharing and Analysis Center (FS-ISAC) (2020): *COVID-19 effects on cybersecurity survey*, July.

Financial Stability Board (FSB) (2017): Stocktake of publicly released cybersecurity regulations, guidance and supervisory practices, October.

Hope, A (2020): "New Zealand Stock Exchange shut down by DDoS cyber attack", CPO Magazine, 3 September.

International Association of Insurance Supervisors (IAIS) (2016): Issues paper on cyber risk to the insurance sector, August.

Microsoft (2020): Security intelligence report, October.

Reserve Bank of New Zealand (RBNZ) (2021): "Reserve Bank responding to illegal breach of data system", 10 January.

Snow (2020): "How the 'new normal' is changing cloud usage and strategy", 16 June.

SWIFT (2019): Three years on from Bangladesh – tackling the adversaries, April.

UK National Cyber Security Centre (NCSC) (2020): Annual Review, November.

US Federal Bureau of Investigation, Cybersecurity and Infrastructure Agency and Office of the Director of National Intelligence (FBI-CISA-ODNI) (2020), "Joint statement", 16 December.

Welburn, J and Strong A (2019): "Systemic cyber risk and aggregate impacts", RAND Corporation, Working Papers, no WR-1311.

ZDNet (2020): "RDP and VPN use skyrocketed since coronavirus onset", 30 March.

Previous issues in this series

No 36 12 January 2021	E-commerce in the pandemic and beyond	Viviana Alfonso, Codruta Boar, Jon Frost, Leonardo Gambacorta and Jing Liu
No 35 15 December 2020	The recession-mortality nexus and Covid-19	Sebastian Doerr and Boris Hofmann
No 34 14 December 2020	Central bank swap lines and cross-border bank flows	Iñaki Aldasoro, Christian Cabanilla, Piti Disyatat, Torsten Ehlers, Patrick McGuire and Goetz von Peter
No 33 02 December 2020	What comes next? Recovery from an uneven recession	Daniel Rees
No 32 12 November 2020	Monetary policy response in emerging market economies: why was it different this time?	Ana Aguilar and Carlos Cantú
No 31 09 October 2020	Bankruptcies, unemployment and reallocation from Covid-19	Ryan Banerjee, Enisse Kharroubi and Ulf Lewrick
No 30 09 October 2020	The outlook for business bankruptcies	Ryan Banerjee, Giulio Cornelli and Egon Zakrajšek
No 29 14 August 2020	Bonds and syndicated loans during the Covid-19 crisis: decoupled again?	Tirupam Goel and Jose Maria Serena
No 28 23 July 2020	Inflation at risk from Covid-19	Ryan Banerjee, Aaron Mehrotra and Fabrizio Zampolli
No 27 16 July 2020	Global banks' dollar funding needs and central bank swap lines	Iñaki Aldasoro, Torsten Ehlers, Patrick McGuire and Goetz von Peter
No 26 01 July 2020	Corporate credit markets after the initial pandemic shock	Sirio Aramonte and Fernando Avalos
No 25 26 June 2020	Investors' risk attitudes in the pandemic and the stock market: new evidence based on internet searches	Marlene Amstad, Giulio Cornelli, Leonardo Gambacorta and Dora Xia
No 24 19 June 2020	Trade credit, trade finance, and the Covid-19 Crisis	Frédéric Boissay, Nikhil Patel and Hyun Song Shin
No 23 17 June 2020	The fiscal response to the Covid-19 crisis in advanced and emerging market economies	Enrique Alberola, Yavuz Arslan, Gong Cheng and Richhild Moessner

All issues are available on our website www.bis.org.