EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Andrea ENRIA
Chair of the Supervisory Board

COURTESY TRANSLATION

Mr Markus Herbrand
Mitglied des Deutschen Bundestages
Platz der Republik 1
11011 Berlin

Frankfurt am Main, 30 April 2021

Re: Your letter of 26 March 2021

Honourable Member of the Bundestag, dear Mr Herbrand,

Thank you for your letter on IT and cyber risk, which was passed on to me by your President, the honourable Dr Schäuble, accompanied by a cover letter dated 29 March 2021. Some of your questions refer to financial market infrastructures. Please note that I can only answer these questions for financial market infrastructures (FMIs) with a banking licence, as only these FMIs are within the remit of ECB Banking Supervision.

Cyber risk has been a supervisory priority for European banking supervision from the onset. The SSM Risk Map for 2021[1] identifies cybercrime and IT disruptions as key risks faced by supervised institutions. But persistent deficiencies in basic cyber protocols, complex information and communication technology (ICT) architecture and a growing amount of end-of-life ICT systems in many institutions still need to be addressed. The challenges for the German banking industry in terms of IT and cyber threats are not very dissimilar to the ones every other bank in the banking union is facing.

ECB Banking Supervision carries out several activities to monitor and address IT and cyber risk faced by banks. First, the cyber incident reporting framework requires all banks that are supervised by the ECB to report significant cyber incidents to us on a confidential basis as soon as they are detected. This allows supervisors to identify and monitor trends and to react quickly if a major cyber incident affects one or more significant institutions Second, ECB Banking Supervision analyses IT risk in every significant institution on a yearly basis in the context of the Supervisory Review and Evaluation Process (SREP). Third, frequent on-site inspections at significant institutions also allow ECB Banking Supervision to assess the IT and cyber risk management capabilities at individual banks.

In this regard, I would also like to refer to the Annual report on the outcome of the SREP IT Risk Questionnaire, which we published in July 2020.[2] The report presents key observations about banks' IT risk

[1] ECB Banking Supervision: Assessment of risks and vulnerabilities for 2021.

[2] Annual report on the outcome of the SREP IT Risk Questionnaire.

European Central Bank
60640 Frankfurt am Main
Tel.: +49 69 1344 0
E-mail: info@ecb.europa.eu
Website: www.bankingsupervision.europa.eu

practices as of the first quarter of 2019. Banks' outsourcing budgets continued to increase throughout 2018 and until the beginning of 2019, with cloud services becoming more relevant. It also describes our supervisory concerns regarding the number of end-of-life systems continuing to support critical business processes, and finds that data quality management remains the weakest risk control domain.

The ECB's supervisory activities follow the EBA Guidelines on ICT and security risk management, which have applied from 30 June 2020. They set out expectations on how all financial institutions should manage the internal and external ICT and security risks to which they are exposed. Looking ahead, the European Commission's proposal for a "Digital Operational Resilience Act" (DORA) is a welcome initiative. It aims to harmonise and streamline existing rules on ICT risk management and ICT-related incident reporting, as well as to introduce new rules on threat-led penetration testing, information sharing and management of ICT third-party risk.

The outbreak of the coronavirus (COVID-19) pandemic has also had an impact on IT and cyber risks. While digital technology has been challenging traditional banking value chains for quite some time, the pandemic has acted as a catalyst to speed up this process. It has highlighted the need for banks to avail themselves of mature digital capabilities to deliver products and services. In this respect, the pandemic has shown that banks under European banking supervision are operationally resilient, even as reliance on remote working has increased significantly. Banks have adjusted their operations to ensure business continuity, thus enabling them to continue providing services on a cross-border basis. At the same time, the pandemic has created additional challenges for banks by moving the focus of these threats. As banks transfer their processes to contingency environments, their exposure to cyber threats increases, as does the risk and impact of IT failures. In particular, banks' IT systems must be resilient enough to withstand the current heavy reliance on remote working and servicing. This has slightly extended the attack surface through the more intensive use of virtual private networks (VPNs) and mobile devices connected to private internet access points. It is therefore vital that banks are aware of the techniques used by those seeking to target their staff working from home, so that they can take adequate measures to mitigate this risk. Banks need to continually adapt their IT and cyber risk strategies and ensure that their staff are aware and have been trained on the risks associated with remote working arrangements. The ECB emphasised this in the early stages of the pandemic in its letter to all significant institutions[3] in March 2020, which included a reference to the need to address the risks of increased cyber security-related fraud in their contingency strategies. ECB Banking Supervision continues to monitor any developments through ongoing supervision and regular monitoring calls with the banks.

As regards your questions on the volume of cyber incidents targeting significant institutions please note that the ECB's Financial Stability Review of November 2020 contains some relevant statistics.[4] Even though the number of cyber incidents reported by significant institutions as increased over time, as of Q3 2020 institutions have not been impacted severely. Cyber incidents reported to the ECB by significant institutions increased somewhat in the third quarter of 2020 and compared with 2019.

[3] See the letter from ECB Banking Supervision to all significant institutions, 3 March 2020.

[4] Financial Stability Review, ECB, Frankfurt am Main, November 2020. Chart 3.9 provides an overview of the evolution of incidents reported under the ECB cyber incident reporting framework in 2019 and 2020, as well as reported cyber incidents by type in 2020.

As for attacks directed at the ECB, the ECB was the victim of a single successful cyberattack – in August 2019. The incident affected the ECB's externally hosted Banks' Integrated Reporting Dictionary (BIRD) website. The business impact was limited to the potential exfiltration of email addresses of subscribers to the newsletter issued periodically by the website. The perpetrators could not be identified, and a press release[5] on the incident was issued at the time.

Yours sincerely,

[signed]

Andrea Enria

[5] See the ECB's press release "ECB shuts down compromised BIRD website" of 15 August 2019.