11 May 2022

In recent years, banks have highlighted time and again that they consider cyber risk to be a key threat to their activities. European regulators such as the EBA and the ECB have also flagged it as a major risk for the sector. Yet cyber risk for banks remains one of the least assessed and considered risk factors.

One of the main reasons cyber risk for banks remains under-assessed is down to the fact that there is hardly any visibility around it, let alone relevant metrics to guide the assessment for specific banks. The market only focuses on it in reaction to a major incident such as a cyberattack or if an IT failure becomes public.

This lack of visibility is explained by the banks' perhaps understandable reluctance to be overly transparent about specific cyber threats and especially about the concrete steps they are taking in cyber security. Detailed disclosure that can help the market assess banks' cybersecurity can also lend a helpful hand to cybercriminals.

Disclosure insufficiencies notwithstanding, this elephant is very much in the room. There are four key reasons why cyber risk has grown into a massive threat for banks:

1 Digital transformation accelerated and broadened exponentially due to Covid-19.

Cyber risk no longer applies to parts of the business; it is now relevant to the quasi-totality of a bank's activities – horizontally (across all front-office and back-office areas) and vertically (from top management down). The more a bank turns digital, the more it is vulnerable to cyber risk.

2 A structural shift in work habits, with pandemic-induced remote working a key trend.

Recent surveys reveal that banks still lack a well-structured cybersecurity culture for their non-technical staff and management. Without a proper cyber defence framework, harmful social engineering techniques using psychological manipulation to trick bank employees into making security mistakes or giving away sensitive information can become easier when they work away from the traditional office structure.

3 The growing world of crypto – currencies, exchanges, and payments – is creating new and dangerous vulnerabilities to cyber threats.

The crypto ecosystem presents new sets of risks. Many of them are still not properly understood or are glossed over in the drive for profits. It is also sub-optimally regulated and supervised, which inherently creates additional risk. As an example, a disproportionately large share of ransomware payments, which are on the rise, is in bitcoins.

4 Geopolitical disruptions, primarily global cyber threats stemming from Russia's war on Ukraine.

On 23 February, a day before the invasion of Ukraine, Russian cybercrime cartels unleashed

Hermetic Wiper, a data-destructive malware targeting financial and other infrastructure. Although focused mostly on Ukraine, the malware has heightened cyberattack concerns around the world. In a statement last March calling on banks to ensure compliance with sanctions against Russia, the EBA stated that "cyber risks are a particular area requiring continued attention".

With respect to adjusting the regulatory framework to include cyber risk (which would also help the market's assessment of it for banks), I highlight two aspects.

First, the need for deeper and more pro-active co-operation across jurisdictions between large banks and their supervisors as well as security agencies. There should be no competitive advantage if one bank suffers a massive and successful cyberattack that spares your bank.

Second, as digitalisation has taken over most of a bank's activities, there should be increased convergence between more traditional supervision of misconduct (including money laundering) and 'pure' cyber risk controls: the combination of technology challenges with financial, legal and human-factor challenges.

"The Golden Age of ransomware"

Exactly three years ago, "The Wide Angle" noted that cyber risk was an existential matter for banks, pointing out also that bank management teams had put in place elaborate structures to enhance cyber resilience[1]. With some success, it seems, as relatively few cyberattacks on large Western banks have occurred or been made public with material market reverberation since then. This was not for a lack of trying by cyber criminals, though.

Rather, it was because the banking industry took the risk seriously and built appropriate defences. And yet, according to experts, the cyber security environment for banks remains filled with threats and uncertainties.

A recent survey of 130 financial institutions worldwide by VMWare, a US cloud-related consultant, revealed that for financial executives, cyber security had become the top issue. Cyber threats and attacks from Russia were viewed as the greatest cyber concern at this time; in addition to an increased use of sophisticated Remote Access Trojan (RAT) threats for ransomware related to remote working. A manager at a large bank claimed that we live in "the golden age of ransomware".

Last year, 63% of banks experienced an increase in destructive attacks – a 17% increase from the previous year. Many banks experienced one or more ransomware attacks (74% of them in one survey), with nearly two-thirds of the victims paying the ransom. Once cybercriminals gain access using a RAT, they can extort the victims or monetise the attacks by stealing resources from cloud services.

The evidence shows that cyber attackers' preferred penetration channel is phishing and other types of social engineering. Which suggests that the weakest cyber-risk link for banks remains the human factor, not the network protection walls. For phishing, sophisticated attackers take advantage of the bank's hybrid work processes and use emotional manipulation tactics on victims. Indeed, to be successful, ransomware and distributed denial-of-service (DDoS) depend on bank staff bending the bank's cybersecurity compliance, willingly or most often unwillingly.

Another technique used by cybercriminals in recent years is "island hopping". Aware that in general banks are by now more adept at protecting themselves against frontal cyberattacks, they go instead after their more vulnerable external partners that are part of the network connected by the bank (e.g. law or accounting firms). Industry data shows that nearly a quarter of cyberattacks on banks make use of island hopping.

[1] https://bit.ly/3L1GwFE

One worrying aspect emerging in recent years is the fact that cybercriminals have gone beyond targeting just payments and transfers, which was the case in the past. They are also focusing on non-public market information (strategies, significant transactions, earnings) which could affect share prices. Two-thirds of large financial institutions have reportedly experienced attacks targeting market strategies. When successful, these can be used to front-run the market or even for economic espionage by private or public rogue actors.

Regulatory focus on cyber risk is catching up

It would be unfair to think that European financial regulators have been ignoring cyber risk. But, not surprisingly, they have not been able to keep pace with the fast advancement of digitalisation, the explosion of new financial products and channels (crypto, blockchain), or the growth of the cybercriminal ecosystem. And, again, Russia and other rogue actors are not going to make life any easier, especially for the larger European banks with internationally widespread operations.

The EBA's guidelines on information and communication technology (ICT) and security risks, finalised at the end of 2019, were intended to address the security risks emerging from the electronic nature of payment services facilitated by the revised Payments Services Directive (PSD2). It is fair to say that at this stage, cyber threats are relevant to more than just payments, as highlighted above, including hacking banks' non-public data too.

In September 2020, the European Commission published a proposed Digital Operational Resilience Act (DORA), which the European Parliament and European Council are still negotiating. It is hoped that a final version will be adopted this year or early next year, with further secondary legislation and technical standards following. Clearly, not a project for tomorrow morning. DORA will address the existing fragmentation in financial legislation and supervisory approaches for digital operational resilience, including cyber.

It will bring critical ICT third-party providers (CTPPs), including cloud-service providers, into the regulatory perimeter of one of the three European Supervisory Authorities (EBA, ESMA and EIOPA). DORA will also set EU-wide standards for digital operational resilience testing and harmonise ICT risk management rules and incident classification and reporting.

Considering a Third Party Provider (TPP) as 'critical' will be a function of the systemic character of the banks relying on its services, as well as on its degree of substitutability. This means that the large cloud-service providers that are critical for the functioning of Europe's financial system will end up being supervised in Europe, at least for related activities. This will be a relevant and necessary accomplishment.

One important step forward in the quest to make cyber risk management by banks and supervisors more effective and transparent was the January 2022 recommendation by the European Systemic Risk Board (ESRB) to establish a pan-European systemic cyber incident co-ordination framework (EU-SCICF)[2]. The ESRB backed its recommendation with a detailed report on mitigating systemic cyber risk, which explains in detail how EU-SCICF would work and what the main benefits would be.

The report also makes suggestions about including cyber risk in the various components of macroprudential policies, including maturity mismatch/illiquidity, limits to exposure concentrations, and resilience of financial infrastructures. If these initial proposals around the EU-SCICF and cyber risk parameters in supervision evolve further, that could lead to a more forward-looking and metrics-based assessment of cyber risk for banks, which would be highly desirable.

[2] https://bit.ly/3kYRSQq

This report is published by Scope Group. The content is an independent view not related to Scope's credit ratings.

Scope SE & Co. KGaA

Lennéstraße 5
10785 Berlin
info@scopegroup.com

Scope Ratings GmbH
Lennéstraße 5
D-10785 Berlin
info@scoperatings.com

Scope Ratings UK Limited
52 Grosvenor Gardens
London SW1W 0AU
info@scoperatings.com

Scope ESG Analysis GmbH
Lennéstraße 5
D-10785 Berlin
esg@scopegroup.eu

Scope Analysis GmbH
Lennéstraße 5
D-10785 Berlin
info@scopeanalysis.com

Scope Investor Services GmbH
Lennéstraße 5
D-10785 Berlin
info@scopeinvestors.com

Scope Hamburg GmbH
Stadthausbrücke 5
D-20355 Hamburg
info@scopehamburg.com

www.scopegroup.com
www.scoperatings.com
www.scopeanalysis.com
www.scopeinvestors.com
www.scopehamburg.com

Disclaimer