SUERF
The European Money and Finance Forum

SUERF Policy Brief
No 343, June 2022

Cybersecurity and financial stability



By Kartik Anand, Chanelle Duley and Prasanna Gai[1]

Keywords: Cyber attacks, bank runs, global games, weaker-link public goods.

As the digital transformation in banking has gathered pace, so have cyber risks to financial stability. The prevalence of cyber attacks is particularly pronounced in the financial system: Data from the Carnegie Endowment for International Peace indicates that the number of cyber attacks on financial institutions is increasing four-fold, year-on-year (Mauer and Nelson, 2020). Together, these trends pose a new challenge for financial sector participants. Despite the growing interest in cyber risk, there is currently no model that links cyber attacks to bank and investor behaviour. This policy brief summarises recent analysis (Anand, et al., 2022) clarifying how cyber attacks can engender financial instability.

[1] **Kartik Anand**: Deutsche Bundesbank, Research Department, Wilhelm-Epstein-Strasse 14, 60431 Frankfurt, Germany; **Chanelle Duley** and **Prasanna Gai**: University of Auckland, 12 Grafton Rd, Auckland 1010, New Zealand.

The views expressed in this paper are those of the authors and do not necessarily represent those of the Deutsche Bundesbank or the Eurosystem, or the New Zealand Financial Market Authority.

> *"Cyber security is a public good… the social benefit conveyed by a well functioning and resilient financial system… requires a higher level of investment in cyber security than what individual firms would like to do on their own. In addition, many individual firms rely on shared services.... an individual firm may rely on others in the shared network to make investments to increase the security of the network, but if every firm thinks this way, there will be underinvestment in security."* – Loretta J. Mester, Reserve Bank of Cleveland, 21 November 2019.

Cybersecurity as a public good

Our analytical framework builds on the premise that banks use shared digital services provided by third-party vendors who offer scale-efficiencies. Examples include data warehousing, runtime services, and operating systems that facilitate both customer online banking services and the bank's back-end operations. Adoption of these services by financial institutions has been accelerating over the past few years (Harmon, 2020). Services are provided by just a handful of companies. A survey by Gartner (2019) estimates that Amazon, Microsoft, Alibaba, Google, and IBM account for 77% of the market.

While cost saving, shared services, which we refer to as "platforms", create cybersecurity dependencies – one bank's access can become the 'back door' through which attackers impact others. By gaining access to a bank's systems, attackers can deploy malicious code to exploit vulnerabilities in the platform – which are often unknown even to the vendor (Perlroth, 2021) – and cause outages. The Stuxnet malicious code that spread via Microsoft Windows and targeted industrial control systems is an example of an attack that exploited several zero-day vulnerabilities (McDonald et al., 2013).

Since remedial actions against vulnerabilities are not always available, banks must, therefore, invest in cybersecurity to monitor and repel unauthorised intrusions into their systems. Investing in cybersecurity allows a bank to protect both itself and others on the platform. Cybersecurity thus has the hallmarks of a weakest-link public good (Hirshleifer, 1983; Cornes, 1993). Just as in times of flood, the sea penetrates the sector where citizens have constructed the lowest dike, the cybersecurity of the financial system depends on the bank with the lowest level of protection. As such, we can picture the "security blanket" over the platform as a circular region with banks situated along the perimeter. Each bank is responsible for maintaining security along its portion of the perimeter. But an attacker who breaches the section of the perimeter guarded by one bank can disrupt the platform and adversely impact all banks. The weakest-link formulation implies that investment in cybersecurity generates positive externalities for all banks.

Cyber attacks

We argue that cyber attacks may be characterised by three factors. First, there is the intensity with which attackers try to breach the cybersecurity defences and causing the platform to suffer an outage. Uncertainty over the intensity of an attack reflects uncertainty about the identity of the attacker - this attribution problem is a distinguishing feature of cyber attacks (Hayden, 2011). For example, state-sponsored attackers have considerable resources to launch more sophisticated attacks that are more likely to be successful than attacks by typical cyber-criminals.

Second, following a successful intrusion and the deployment of malicious code, the shared services may suffer temporary outages that disrupt operations for all banks. For example, the recent distributed denial of service (DDoS) attack on the New Zealand Stock Exchange prevented the posting of market announcements and led to trading suspensions over several days (Tarabay, 2021). During these outages, banks are unable to access or manage some proportion of their key functions.

Third, even after the attack has been repelled, there may be longer-lasting damage. These include the loss of secret information pivotal to the bank's role as a financial intermediary (Dang et al., 2017), losses incurred from paying ransom demands, and even physical damage to critical systems. Bouveret (2018) estimates that the annual average loss to banks from cyber attacks amounts to some US$100 billion, or 9% of banks' net income globally.

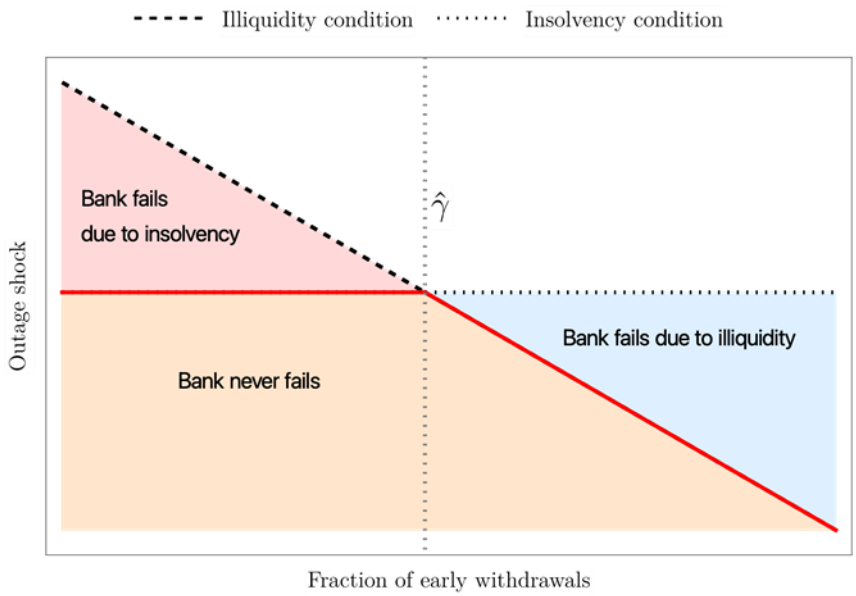
Bank illiquidity and insolvency conditions

Platform outages can impair a bank's ability to manage its assets and, thereby, service its debts in a timely manner. In particular, if the outage is sufficiently large, relative to the mass of debt holders who choose to withdraw, this can render the bank illiquid but solvent. The decisions of debt holders to withdraw are, in turn, driven by their concerns over the bank's ability to pay. In our model, we parametrise these concerns by the degree of rollover risk.

Cyber attacks can also lead to banks suffering financial losses. The credit downgrading in 2019 of the Maltese bank, Valletta PLC, following a cyber attack highlights the risks to bank insolvency (S&P Global Market Intelligence, 2019). If the losses are large, they can lead to banks failing due to insolvency.

Figure 1 depicts how the insolvency and illiquidity conditions of a bank – following a successful cyber attack – are related. While the insolvency condition only depends on the severity of the outage shock, the insolvency condition depends on both the outage shock and mass of debt holders who withdraw. Importantly, there is a critical mass of withdrawals, denoted γ, at which the two conditions intersect. Whenever withdrawals are less than γ, then bank failure is primarily driven by insolvent. While, when the mass of withdrawals is greater than , concerns over illiquidity are the overarching reason for the bank to fail, even though it may be solvent.

Figure 1: Bank insolvency and illiquidity conditions following a successful cyber attack



Banks' investments in cybersecurity and operational resilience

Banks can protect themselves from cyber attacks by investing in cybersecurity. The more banks invest in cybersecurity, the more capable they become at detecting and thwarting unauthorised intrusions. These investments include the hiring of IT specialists to continually monitor systems, providing phishing awareness and general IT security training to staff, engaging in threat sharing activities, and purchasing tools and applications such as unified threat management (UTM) systems.

Banks can also invest in business continuity in the event of an outage to shore up their operational resilience. Unlike cybersecurity, which is a public good, operational resilience is a private good, the benefits of which are not shared with other banks. Investment in business continuity reduces the proportion of bank operations that are temporarily suspended in the event of an outage. Survey results from Accenture (2019) indicate that banks spent up to 29% of their cybersecurity budget on discovery activities in 2018, compared to 18% spent on recovery operations in the event of an outage.

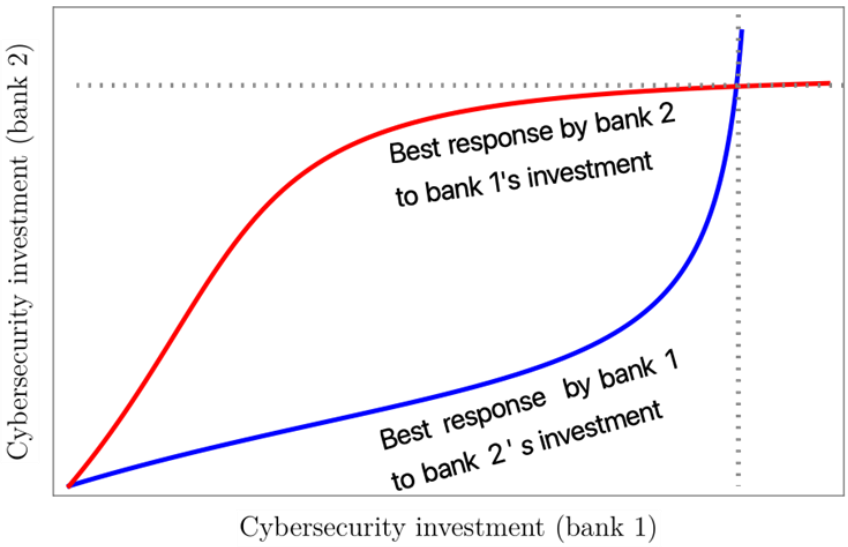
Trade-offs

From the perspective of an individual bank, by investing more in cybersecurity, it contributes towards improving the security blanket around the platform, thereby lowering the probability of a successful attack for all banks. But, this comes at the cost of reducing its investment in operational resilience, which makes the bank more likely to fail in the event of a successful cyber attack. Moreover, as the degree of rollover risk increases, the benefits of greater operational resilience are reduced as debt holders are more likely to withdraw en-masse even when the outage is less severe. It is therefore optimal for the bank to invest more towards cybersecurity and thwart cyber attacks as the degree of rollover risk increases.

At the system-level, two outcomes emerge. In the first, if a bank anticipates that others will invest more their own operational resilience, it expects the level of cybersecurity to be low. It is therefore a best-response for the bank to also invest more towards operational resilience. Since all banks reason in this way, there is no investment in cybersecurity in this "bad" equilibrium.

In the "good" equilibrium, each bank invests unto the point that it optimally trades off shoring up cybersecurity and its own operational resilience, given what it anticipates for the investments of other banks. Figure 2 depicts the two outcomes for the case of two banks where each curve is the optimal level of investment in cybersecurity by a bank given what it anticipates the other bank invests.

Figure 2: Intersections of banks' best-response correspondences denote the equilibria



Since each bank does not internalise how its investment choices influences that of other banks, this given rise to free-riding incentives. To this end, we compare the banks' cybersecurity investment decisions with those of a social planner, who accounts for how each bank's decisions influences those of others. We find that free-riding leads to an underinvestment in cybersecurity by banks relative to the social optimum chosen by the planner. Moreover, as rollover risk increases, not only do the bank's choose to invest more in cybersecurity, but so too does the planner. Consequently, the extent of underinvestment in cybersecurity is exacerbated.

Policy tools

Regulatory and supervisory tools that account for how ex ante free-riding incentives interact with ex post run risk for banks may be used to implement socially optimal cybersecurity investments. Our paper provides new perspectives on tools currently being used by regulators and the industry.

First, regulators can improve banks' incentives to invest in cybersecurity by establishing negligence rules. A negligence rule works by setting the socially optimal solution as a minimum level of due care for each bank (Brown, 1973; Shavell, 2009). If a cyber attack is successful and banks suffer losses, then there is no further liability as long as all banks exercise the due care standard. Otherwise, banks that exert insufficient care are penalised proportionally to the level of their under-investment with a penalty. The ability of the US Securities and Exchange Commission (SEC) to sanction and fine financial firms for deficient cybersecurity procedures is an example of such a negligence rule. In 2021, the SEC fined eight firms $200,000 – $300,000 each for poor cybersecurity that resulted in the disclosure of customer information.

Second, regulators can achieve the social optimum outcome by requiring that banks invests accordingly on an ongoing basis (i.e. before any cyber attacks take place). Such investment can be elicited through cyber hygiene notices and stress tests. Clearly, monitoring and supervising banks' cybersecurity activities will elicit greater investments. But this may come at the expense of subordinating banks' investment choices in the interest of the public good. An example is the approach taken by the Monetary Authority of Singapore (MAS).

The MAS sets minimum regulatory guidelines in the form of a Cyber Hygiene Notice that obliges banks to implement a set of cybersecurity measures, including network perimeter defenses, malware protection, and

baseline configuration standards. Compliance with these regulatory requirements and expectations are verified and enforced by the MAS (Goh et al., 2020). The use of cyber stress tests, such as those implemented by the Bank of England, is another form of such a regulatory approach. The Financial Policy Committee of the Bank tests the resilience of the UK financial system to cyber attacks by requiring financial firms to meet a system-wide tolerance threshold set by the regulator (Kashyap and Wetherilt, 2019).

Conclusion

Financial regulators are increasingly focussed on cyber risks to financial stability. For example, the European Central Bank has introduced a Threat Intelligence-Based Ethical Red Team (TIBEREU) framework for EU-based financial entities (Panetta, 2020). And the Monetary Authority of Singapore has examined how banks' capital and liquidity buffers might cope in the face of a 24-hour system outage triggered by a cyber event (Goh et al., 2020). Our analysis provides a formal basis for such regulatory emphasis and highlights the importance of data on network linkages between banks and digital platforms. Such data might usefully inform "top-down" macroprudential cyber stress testing in much the same way as stress tests on interbank networks (Gai et al., 2011; Glasserman and Young, 2016).

References

Accenture (2019). The cost of cybercrime. *Accenture Ninth Annual Cost of Cybercrime Study*.

Anand, K. Duley, C. and Gai, P. (2022). Cybersecurity and financial stability. *Deutsche Bundesbank Discussion Paper No. 08/2022*.

Brown, J. P. (1973). Toward an economic theory of liability. *The Journal of Legal Studies 2*(2), 323–349.

Bouveret, A. (2018). Cyber risk for the financial sector: A framework for quantitative assessment. *International Monetary Fund, Working Paper No. 18/143*, Washington DC.

Cornes, R. (1993). Dyke maintenance and other stories: Some neglected types of public goods. *The Quarterly Journal of Economics 108*(1), 259–271.

Dang, T. V., G. Gorton, B. Holmström, and G. Ordonez (2017). Banks as secret keepers. *American Economic Review* 107(4), 1005–29.

Duffie, D. and J. Younger (2019). Cyber runs. *Hutchins Center Working Paper 51*, Brookings Institution.

Gartner (2019). Forecast: Public Cloud Services, Worldwide, 2017-2023, 3Q19 Update.

Glasserman, P. and H. P. Young (2016). Contagion in financial networks. *Journal of Economic Literature 54*(3), 779-831.

Goh, J., H. Kang, Z. X. Koh, J. W. Lim, C. W. Ng, G. Sher, and C. Yao (2020). Cyber risk surveillance: A case study of Singapore*. MAS Staff Paper No. 57*.

Harmon, R. (2020). Cloud concentration risk: A framework agent based model for systemic risk analysis. *Journal of Financial Compliance 4*(3): 232-256.

Hayden, M. (2011). Statement for the Record, House Permanent Select Committee on Intelligence, The Cyber Threat. National Security Agency. Available at https://www.hsdl.org/?view&did=689629

continued

Hirshleifer, J. (1983). From weakest-link to best-shot: The voluntary provision of public goods. *Public Choice 41* (3), 371–386.

Kashyap, A. K. and A. Wetherilt (2019). Some principles for regulating cyber risk. *AEA Papers and Proceedings 109*, 482–87.

Mauer, T. and A. Nelson (2020). International strategy to better protect the financial system against cyber threats. Technical report, Carnegie Endowment for International Peace.

McDonald, G., L. Murchu, S. Doherty, and E. Chien (2013). Stuxnet 0.5: The missing link. Symantec security response, Symantec.

Mester, L. J. (2019). Cybersecurity and financial stability. Speech at the Federal Reserve Bank of Cleveland, Cleveland, Ohio. 21 November.

Panetta, F. (2020). Keeping cyber risk at bay: our individual and joint responsibility. Introductory remarks at the fifth meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures. Frankfurt, 16 December.

Perlroth, N. (2021). *This is how they tell me the world ends: The cyberweapons arms race*. Bloomsbury Publishing.

Shavell, S. (2009). *Economic analysis of accident law*. Harvard University Press.

S&P Global Market Intelligence (2019). S&P downgrades Malta-based Bank of Valletta. Available at: https://www.spglobal.com/marketintelligence/en/news-insights/trending/5mvfiykwlxliliri78qd-q2.

Tarabay, J. (2021). How a dated cyber-attack brought a stock exchange to its knees. *Bloomberg Businessweek*.

About the authors

Kartik Anand *is an Economist within the Research Centre at the Deutsche Bundesbank. His research interests include topics in banking, cybersecurity, and sovereign debt.*

Chanelle Duley *is a PhD Candidate at the University of Auckland, New Zealand. Her research interests include topics in money and banking, international economics and political economy.*

Prasanna Gai *is Head of the Department of Economics and Professor of Macroeconomics at the University of Auckland. His work, which applies ideas from network and game theory to understand the causes and consequences of financial crises, has been published in leading journals, including The Review of Financial Studies, Economic Journal, Journal of Monetary Economics, Journal of International Economics, and the Proceedings of the Royal Society (A). Professor Gai is also the author of two books on financial crises and systemic risk, both published by the Oxford University Press. He holds a Doctorate and a Master of Philosophy (Economics) from Christ Church, Oxford, and a Bachelor of Economics (Hons) from the Australian National University. Professor Gai serves on the Board of the New Zealand Financial Markets Authority, is a Senior Research Fellow at the Deutsche Bundesbank, Frankfurt, an Academic Adviser to the Bank of Canada, Ottawa, and a Fellow of the National Institute of Social and Economic Research (NIESR), London, Britain's oldest independent economics thinktank.*

SUERF Publications

Find more **SUERF Policy Briefs** and **Policy Notes** at www.suerf.org/policynotes

SUERF
The European Money and Finance Forum

SUERF is a network association of central bankers and regulators, academics, and practitioners in the financial sector. The focus of the association is on the analysis, discussion and understanding of financial markets and institutions, the monetary economy, the conduct of regulation, supervision and monetary policy.

SUERF's events and publications provide a unique European network for the analysis and discussion of these and related issues.

SUERF Policy Briefs (SPBs) serve to promote SUERF Members' economic views and research findings as well as economic policy-oriented analyses. They address topical issues and propose solutions to current economic and financial challenges. SPBs serve to increase the international visibility of SUERF Members' analyses and research.

The views expressed are those of the author(s) and not necessarily those of the institution(s) the author(s) is/are affiliated with.

SUERF Secretariat
c/o OeNB
Otto-Wagner-Platz 3
A-1090 Vienna, Austria
Phone: +43-1-40420-7206
www.suerf.org • suerf@oenb.at