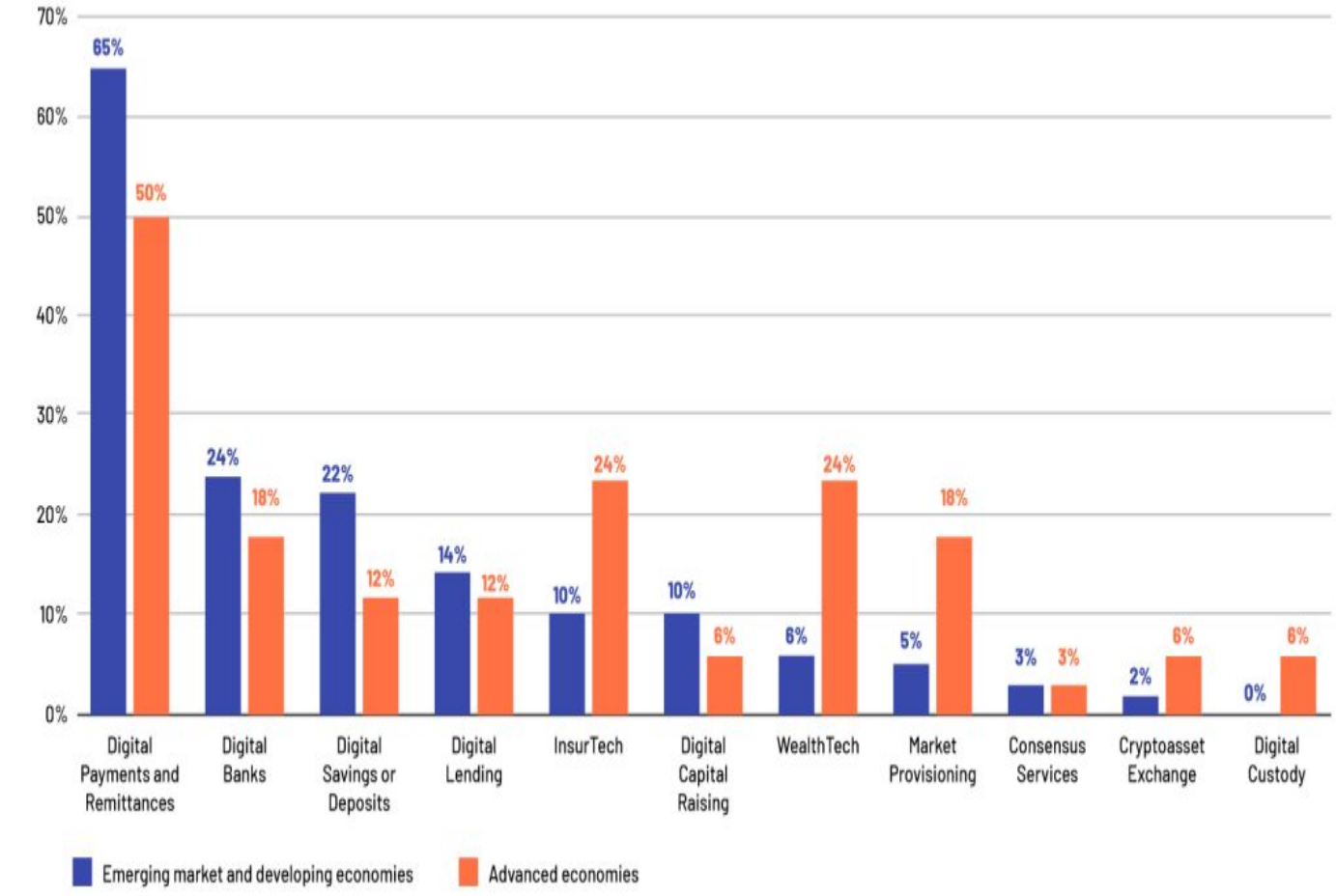
Digital operational resilience for the financial sector and amending regulations

Anvitha R Jain and Jeevitha Jaganatha

Introduction

Digital Innovation is transforming financial services. With innovation in financial technology like growth in Fintech, use of Blockchain, increase in the use of digital wallets and crypto-assets have emerged around the world, meanwhile, artificial intelligence, cloud service, and distributed ledger technology (DLT) are modifying markets in areas as diverse as financial markets. The COVID pandemic has accelerated the digit transformation. In specific the need for digital connectivity to replace physical Interaction between the customers and provider, the ideal approach has been applied to financial payments, retail banking, insurance, and wealth management in financial service. With an increase in digitization, cybersecurity threats have also gained more limelight in recent days bringing greater attention to the need for **cybersecurity financial services**.

In emerging and advanced economies, the percentage of regulators who reported an increase in Fintech usage or offerings as a result of COVID-19.



Source: World Bank and Cambridge Centre for Alternative Finance, 2020.

According to a World Bank and Cambridge Center for Alternative Finance poll done in 2020, there will be a significant move to digital financial services, particularly for payments. Regulators saw a 65 percent growth in digital payments, followed by a 24 percent increase in digital banking, a 22 percent increase in savings, and a 14 percent increase in loans.

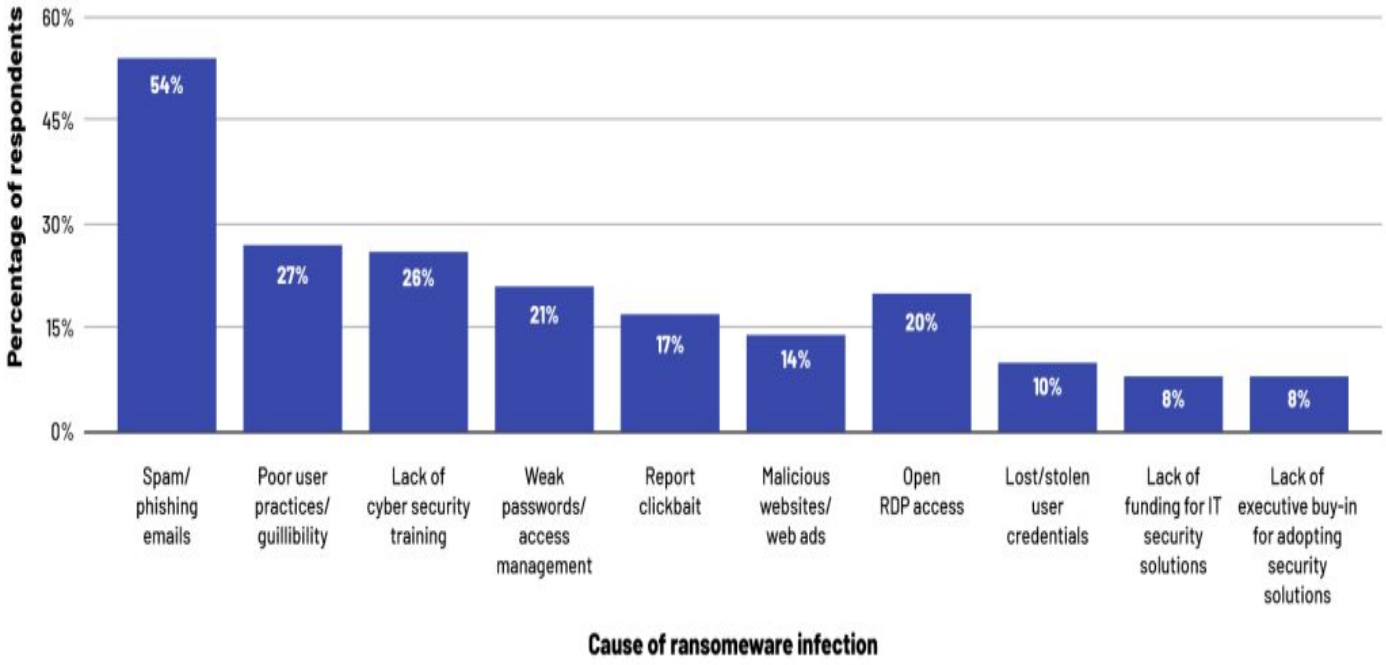
Information and Communication Technologies

Globalization has led to a rise in advanced technology in many countries which makes electronic finance an important aspect for financial sectors. Information and Communication Technologies (ICT) refers to a wide range of Information services that address and manage electronic information. Several sectors have been able to maintain a competitive advantage in the global market thanks to innovative services provided by the information technology sector in recent years.

The growth in digital innovation and advanced technology like ICT has led to an increase in Cyber security threats and cybercrimes. In finance, cybercrime refers to profit-driven criminal conduct such as identity theft, ransomware assaults, email and internet fraud, and financial account manipulation.

Cybercrimes are increasing at a rapid rate. In line with research, the cost of cybercrime will Increase 15% once a year to exceed US$10.5 trillion by 2025. Currently, the bigger part of cybercrime is ransomware and multi-pronged attacks that capture an organization's data and systems and concurrent extortion threatening to release the company's data unless additional payments are made. One such case took place in late March 2021 with a leading Insurance Company based in the USA which paid $40 million to regain control of its network over a ransom cyberattack. (Source: Bloomberg, https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack)

Most common delivery methods and cybersecurity vulnerabilities causing ransomware infections according to MSPs (Management service providers) worldwide as of 2020



Statistic shows the primary reasons of ransomware infections according to MSPs worldwide in 2020. According to the report, phishing scams were the most common cause of ransomware infection for 54% of responding MSPs.

Cybersecurity is one of the highest risks faced by financial institutions so there are more stringent regulations associated with cybersecurity to scale back and mitigate risk. One such initiative is taken by the European Commission called Digital Regulations Resilience for the financial sector and amending regulations (DORA) which mainly focuses on:

- Digital finance strategy
- Proposal for a regulation on markets in crypto-assets

- Regulation on the pilot regime for market infrastructure based on distributed ledger technology (DLT)

(Pilot regime address issue related: it recognizes the potential need for regulatory change in light of new technologies, identify areas that may be insufficient innovation-friendly and seeks to create DLT market infrastructures to prove that existing EU rules are contradictory with DLT)

- Derive to clarify or amend certain related EU financial services

- To establish oversight framework for critical ICT (Information and Communication Technologies) third-party providers

DORA strives to improve and update existing norms and regulations related to digital operational resilience, such as ICT governance, ICT risk management, incident reporting, and ICT third-party risk, which were previously limited.

Introduce new requirements where gaps exist, including a framework for important ICT third-party service providers to monitor digital hazards, information exchange, digital testing, and management of ICT third-party risk.

DORA is looking forward to supporting digital finance in terms of assuring competition, innovation, technology testing, and actions to better enable and enhance the promise of digital finance while limiting risk.

According to the proposal, all the financial entities regulated at the Europe level would be considered

- Financial entities: Include, but not limited to, credit and payment institutions, electronic money institutions, investment firms, crypto-asset service providers, alternative investment fund managers, management companies, insurance undertaking and intermediaries, credit rating agencies, audit firms, securities, trade and securitization repositories, crowdfunding service providers.

- ICT third-party service providers: Include, but are not limited to, cloud computing services, software, data analytics, and data centers.

The main obligation of the DORA proposal are as follows:

1. ICT Risk Management:

- Risk management framework ensures that all financial entities have a sound, comprehensive, and well-documented framework that includes identification, detection, protection/prevention, and response/recovery. Management who would be in charge of controlling the financial entity's ICT risk should use such frameworks.

- Financial institutions should utilize and maintain reliable ICT systems to conduct their operations, allowing them to detect odd activity and identify every type of ICT risk on a regular basis.

2. ICT-related incidents:

- **Financial organizations must design and implement ICT-related incident management processes to monitor, detect, manage, and communicate ICT-related incidents, as well as classify and apply early warning indications as alerts, depending on criteria.**

- **To allow financial regulators to better assess the frequency, nature, and impact of all major ICT-related disruptions, financial firms shall classify ICT-related indents and report important ICT-related incidents to the central EU hub within stipulated timeframes.**

3. Digital operational resilience Testing:

Financial institutions should conduct digital operational testing on a regular basis to identify weaknesses, inadequacies, and gaps in their digital operational resilience, and ensure that corrective measures and tests are carried out by third parties (both internal and external)

4. Information sharing arrangements (Article 40)

- Financial entities may exchange cyber threat information and intelligence among themselves only when the financial entity notify competent authorities about the participation in the information-sharing arrangement.

- Information-sharing agreements protect the sensitive nature of the information given and are governed by norms of conduct that maintain company confidentiality to the fullest extent possible. As a result, confidential information is protected and situational awareness is increased.

5. Managing ICT third-party risk

- Financial entities are held responsible to manage the ICT third-party risk.

- Financial entities get all the information with regards to the regulations, laws, The framework of ICT third-party management takes care of contractual agreements of third-party by providing supervision as to which they meet the requirement from Article 27 of DORA.

- The critical steps taken towards the inspection of third-party include audits and supervision. It is undertaken in order to avoid breach of European Supervisory Authorities (ESAs) guidelines. These guidelines of ESA are the instructions developed from the joint committee and they also contain regulatory standards.

- Hereby the ICT third party is mandatory to disclose a clear and complete description of the contract including all the other required information such as the location of service provider, performance targets in order to be easily monitored by financial entities.

- On account of breach of any regulations or any misleading activity identified and reported then the lead overseer from the following authorities listed below are responsible to inspect online and off-line.

- The European Banking Authority (EBA)
- The European Securities and Markets Authority (ESMA)
- The European Insurance and Occupational Pensions Authority (EIOPA)

- The financial entities in order to conduct an investigation, collect all the required documents as per articles 32, 33, 34, and 35 which contain guidelines regarding the request of information, general investigation, and oversight and following up and also charging the fees for oversight respectively.

- In regards to penalties overseer has the right to impose administrative penalties and criminal penalties.

Conclusion

Although DORA is still in the works, it would be a much-welcomed update that reinforces the financial sector's existing laws regarding digital operational resilience.

This in turn reduces the risk related to cyber security and risks arising from third-party management.