ANALYSIS

# Financial sector also facing new kinds of threats

Financial stability | 13.05.2022 | Pasi Miettinen

AUTHOR

Pasi Miettinen
Senior Economist

Payment systems are part of the key infrastructure for Finland’s national preparedness. The financial sector is part of the chain of national preparedness that must not be allowed to break even during an emergency. National contingency planning for payments is therefore necessary in order to create effective backstops for exceptional situations of different kinds. Sufficient contingency planning will help ensure that confidence is retained even during disruptive situations.

## Foresight and training are essential in contingency planning

Banks and other payment service providers switched to using pan-European payment infrastructures in the early 2000s. The efficiency benefits of these arrangements are undisputed, and the use of these systems in global interaction is often essential. Some of the processes of individual banks have also been transferred to operating units located abroad or to foreign subcontractors. Long-term disruptions to these processes would have a considerable impact on the functioning of payment traffic and securities business in Finland.

The financial sector and other critical sectors regularly practice[1] preparations for dealing with disruptions and incidents of various kinds. Through these exercises, participants gain necessary information on the strengths and weaknesses of the sector and their own organisation. These exercises provide an overview of how the materialisation of current threats would affect the sector, and also provide an opportunity to develop resilience in the sector. Training is not enough in itself, however, as decisions taken in conjunction with it must also be put into practice within the sector and at the level of individual market operators.

In the financial sector training, it has long been recognised that there are vulnerabilities in Finland's payment infrastructure. Although Finnish market operators have invested in incident management and, among other things, in improved prevention of cyber threats, contingency planning for the sector as a whole is inadequate.

## Growing range of threats

Damage to the communications cables connecting Finland with the rest of Europe, and the consequent loss of connections to systems and services located beyond Finnish borders, has traditionally been seen as the biggest threat to the financial sector.

Individual cyber attacks are commonplace. Short-duration DoS (denial of service) attacks, phishing attempts and malicious hacking have been widely covered in the media. They have not so far had any major impact on critical functions in Finland. However, cybercrime perpetrators are no longer just individuals and amateurs but now include organisations and government actors. Such entities have at their disposal top-class expertise and considerable resources. The motives behind their actions have traditionally been financial gain, causing harm and thrill-seeking. Cyber attacks may also be conducted as part of hybrid interference. To guard against cyber attacks and other continuity disruptions, it is vital to consider what to do in the event that protective arrangements fail, and how to revert to normal once the situation has passed.

Even where an individual market operator is able to protect itself effectively from cyber risks, the sector as a whole may have serious shortcomings. Many firms have outsourced part of their activities. Outsourcing may have allowed them to improve efficiency and to share with others the costs of investing in new technologies. The use of cloud computing services, for example, has become more widespread in recent years in all sectors. However, outsourcing can be difficult to manage if the outsourcing chains are long and the view of the big picture is blurred.

## Critical sectors’ interdependency risks as technology advances

Different sectors are networked with each other, and so a vulnerability in one sector can lead to vulnerabilities across a whole chain or even to wider problems. As an example, problems in power generation or in communications will have an extensive impact on society, including the financial sector. Problems in the financial sector could then be reflected in e.g. retail payments. Recognising interdependencies and making contingency plans for each chain is especially important, because the whole is only as strong as its weakest component.

We have become increasingly dependent on the reliable functioning of communications networks. Maintaining access to databanks has also become critical. Disruptions in communications networks will have an impact on other sectors. It is not enough merely to duplicate operational systems as a way of planning for contingencies. Instead, there has to be a clear plan for ensuring that communications networks and databanks are still available during disruptions.

Our globally networked world is making increasing use of technologies. This should be done efficiently and securely. These developments are, for the most part, positive, and they have allowed us to be part of a global picture, but at the same time our scope for influencing matters at national level has diminished.

## How do we pay in emergency situations?

Payment is one of the essential functions in society. It is vital that salaries, pensions and benefits can be paid, and that people can buy essentials for living, such as food, medicine and power. The systems used for payment must be secure, reliable and efficient. If the use of these systems is prevented for some reason, payments that are essential for the functioning of society must be managed in some other way.

A target level which is suitable and sufficient must be set for this in contingency planning. Not all services used in normal conditions are necessary in prolonged disruptions or emergencies. Instead, preparedness must focus on essential needs, which is also important from a cost-effectiveness viewpoint.

The operation of financial markets is based on confidence. A disruption to payments or to the transmission of payments could cause a loss of confidence in the banking system, especially if the disruption is prolonged. Sufficient contingency planning will help ensure that confidence is retained even during disruptive situations.

## Notes

1. E.g. the FATO21 and TIETO22 exercises. ↑

## Key words

contingency planning, financial sector, payment systems, settlement systems, threats