Could a cyber attack lead to financial crisis?

9 Jun 2015 – Analysis – Financial stability

Otso Manninen
Senior Economist

If loss in interbank confidence regarding banking sector balance sheets intensified the crisis in 2008, banks' faltering confidence in other banks' systems could cause the next crisis, experts warn. Confidence is vital to the financial system, and as account balances are situated in cyberspace, confidence in the numbers on the screen is of the utmost importance. From a practical point of view it is irrelevant whether a loss of confidence is due to the realisation of financial market risks or cyber risks.

Digitalisation has revolutionised the entire financial system

The financial sector is a pioneer in digitalisation: securities markets and most payments are handled electronically. Digitalisation has already revolutionised the entire banking sector, and there is no end in sight to this development. The change has mainly been positive, making banking services more easily accessible and increasing competition between service providers. Digitalisation has, however, brought about a new type of risk: cyber crime.

At the turn of the year many in Finland found that online banking was inaccessible, card payments could not be made and cash withdrawals from ATMs did not work. Although downtimes only occurred during a few days, this undermined confidence in the entire system: it's a problem for users if they cannot trust that payments can be made on time. However, a short denial-of-service attack against an individual bank does not yet affect the stability of the entire financial system.

More serious cyber attacks against financial institutions, or particularly against the financial infrastructure, can already affect the real economy and confidence in market participants directly. While, earlier, continuity in system operations was in the interest of a cyber criminal who had accessed user codes via phishing, a modern cyber criminal may aim at causing disruptions that are as serious and sustained as possible. This creates a link between cyber security and financial stability.

Cyber security maintains financial stability

Cyber security is part of financial stability, but heretofore cyber attacks have not been taken into account as a possible origin of financial crises. The probability of problems from a cyber attack spreading into a crisis testing the whole financial system is still fairly small compared with many other risks. As a result, cyber security is still not the first priority when assessing macro stability risks. However, a significant difference compared with many other systemic risks is that some cyber criminals may have a clear incentive and tools to try to cause a crisis.

Since the previous financial crisis, authorities and legislators have produced more detailed and precise regulations for banks and other financial institutions. The purpose of the new regulations has been to decrease the probabilities of financial crises, lower the social costs of crises and in general terms strengthen confidence in the financial sector. If they work as intended, the new regulations will lower the probability and costs of financial crises. However, crises can often arise from unexpected situations.

Although a cyber attack may cause no systemic risk as such, it could cause disruptions indirectly. According to a recent estimate, losses of GBP 20 billion could arise in the insurance sector from payment of cyber insurance compensation.[1] If the volume of cyber insurance increases, the largest possible cyber loss could outstrip the corresponding sum for a natural catastrophe. Between financial institutions closely linked through IT systems, a cyber attack could spread from one system to another and increase the probability of large indemnities, thus jeopardising the loss resilience of the insurance sector.

Authorities recognised importance of cyber security

During the past couple of years, central banks, financial market supervisors and legislators have emphasised the importance of cyber security. Financial institutions have

1. See the report of HM Government and the Marsh Insurance Company: 'UK cyber security: the role of insurance in managing and mitigating the risk', at https://www.gov.uk/government/news/cyber-security-insurance-new-steps-to-make-uk-world-centre.

already had to take cyber security into account, but increasing awareness and consideration of existing cyber risks are still important areas of development.

In the Bank of Finland's oversight work and the Finnish Financial Supervisory Authority's supervision, the importance of financial institutions' cyber security will be increasingly emphasised. Cyber security comprises many sub-areas over and above technical IT systems. It is an umbrella concept including business practices, staff training as well as clear communication and operating plans in case of a cyber attack. Supervisors and overseers aim to assess this comprehensive cyber security and direct it towards the best possible practices.

Best cyber security practices are developed at international level. At the end of 2014, the Bank for International Settlements (BIS) published its first report on cyber security and how financial institutions should take cyber security into account in their own operations.[1] Each institution and country is different, and international recommendations can only address commensurate activities. For this reason, financial institutions must take active steps to develop their own cyber security.

Cyber security affects public confidence in the financial system. However, this is a far cry from disrupted financial stability. So far regulators and supervisors have aimed to make financial institutions resilient against financial crises. Increasingly tighter capital requirements, larger collateral, better risk models and many other changes have been part of this process. Next, we must ensure the invulnerability of our IT systems. Comprehensive cyber security must be taken seriously, so that the next crisis does not start from where experts warned it would.[2]

Tags

digitalisation, financial stability, cyber security, financial market infrastructure

2. See the report 'Cyber resilience in financial market infrastructures', at http://www.bis.org/cpmi/publ/d122.htm.