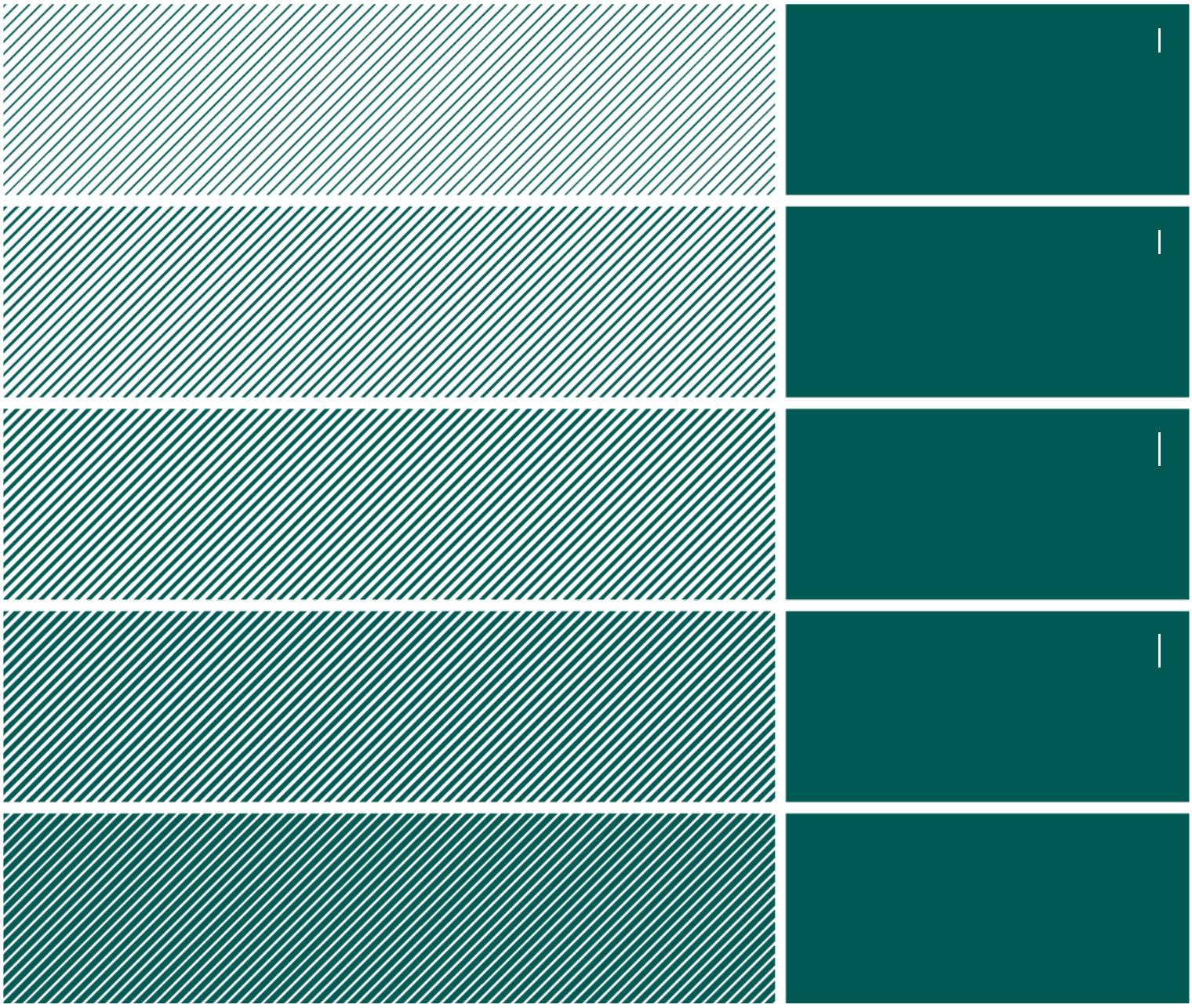
FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Report

Risk and Vulnerability Analysis 2012

Financial Institutions' Use of Information and Communications Technology (ICT)



Risk and Vulnerability Analysis (RAV) 2012

Financial Institutions' Use of Information and Communications Technology (ICT)

Finanstilsynet, April 2013

Contents

1 Introduction

Finanstilsynet (the Financial Supervisory Authority of Norway) performs an annual risk and vulnerability analysis (RAV analysis) of the financial sector's use of ICT and payment services. The report is based on data from a number of internal and external sources, and contains assessments of how identified risks can impact the financial sector in Norway. Technological developments and the financial sector’s introduction and use of increasingly complex services makes work relating to risk more demanding for both the individual institution and the authorities. New technology often contains unknown vulnerabilities, which during the early phase can be both exploited by criminals and result in failures.

The internet opens the way for global electronic crime, or cybercrime. If the financial sector is to be at the forefront of these developments, it must have access to correct information on international trends and systems for handling and reacting to undesired incidents, both legally and technologically.

In order to understand what may give rise to higher risk in the future, it is important to have the facts of the risk situation and to be capable of determining which factors may change over time and result in higher risk. The aim of Finanstilsynet's annual RAV analysis is to provide a picture of developments in the risk associated with the financial sector's use of ICT and payment services.

1.1 Summary

Losses on payment services increased in 2012, above all on internet banking. However, losses remained relatively low despite the increase over 2011.

There was also an increase in criminal attacks on payment services, particularly on internet banking and payment card use on the internet. There was an increase in DDOS attacks (Distributed Denial of Service Attack) in 2012.

The clearing and settlement systems showed a high level of stability in 2012. Although some critical incidents were noted, stability was satisfactory over the year as a whole. The banks need to be clearer to customers about the expected availability of the internet banking solutions. The customers' appear to expect round-the-clock access, yet this is not stated in the agreements between the banks and their customers. One critical incident occurred at the Norwegian CSD related to deletion of data at the securities register, but this was corrected in a satisfactory way.

Chapter 2 summarises risk issues and upcoming legislation and recommendations.

Chapter 3 covers the payment systems, which represent a large portion of the banks' business. The chapter assesses the general risk level, critical incidents in the payment systems and developments in criminal activity against the payment systems. It also provides statistics of losses in the payment systems for 2011 and 2012.

Chapter 4 describes findings and observations made by Finanstilsynet in 2012. They mainly derive from inspections, reported incidents, interviews with selected institutions and inspections conducted at ICT service providers.

Chapter 5 covers areas Finanstilsynet considers to pose the highest risk. These are:

- management and control
- attacks on internet-based systems
- business continuity and disaster recovery solutions
- risk associated with old and complex systems
- access to payment services

Chapter 6 describes measures Finanstilsynet will continue to focus on in relation to the risk areas described in chapter 5.

2 General trends

It is challenging to keep up with developments in technology, service providers, computer crime and national and international rules that may influence the risk picture. Failure to understand and follow up on these issues may result in increased risk, so it is important that developments be monitored to ensure that a situation that is constantly changing can be handled satisfactorily.

2.1 Private equipment

Employees in both the public and the private sector increasingly use their own private mobile devices (BYOD: Bring Your Own Device") for work-related purposes. However, surveys undertaken by Finanstilsynet of financial institutions in Norway indicate that they are very restrictive about allowing BYOD. If the security rules established by an institution for its work stations do not apply to private equipment, the institution's internal network must reject private equipment when attempts are made to connect it to the network. The institution should then see private equipment as a threat, to be countered by such measures as antivirus software, firewalls, IDS, IPS and Trojan signatures.

The institution must check whether the security of private equipment has been updated before this equipment is allowed to communicate in the institution.

Private equipment has gradually acquired substantial storage and processing capacity, so it is feasible to transfer a financial institution's data and programs to private equipment. It is important that the institution has sound procedures for logging such activity. This is a general measure to prevent data theft, but the introduction of private equipment makes the problem more urgent.

Financial institutions should have procedures that make it mandatory for employees to report lost equipment and give the institution the right to delete any of the institution's data that might be stored on the mobile device via the network, if this is possible.

One unprotected computer in a network is enough to allow unauthorised persons to secure "control" of a network. Automated search programs make it simple to detect unsecured elements. It is therefore important to have a good overview of the computers in the network. Computers that are seldom used and back-up equipment must also be updated according to the general security procedures.

2.2 Identity theft

Finanstilsynet uses the term ‘identity theft’ when someone has dishonestly obtained personal data that are abused in order to secure financial advantage or other benefits without the knowledge of the rightful owner. Identity theft takes place by the person in pursuit of the identity:

- taking control of the user by means of overlay services, phishing, Trojans or theft of ID papers,

- pretending to be a bank with the aid of Trojans, false certificates, false websites, copied logos etc.,
- taking over the network with the aid of programs that send the customer to the attacker's website instead of the bank's – also known as domain name system (DNS) poisoning.

It is very simple today to copy pictures, text and websites. Attackers use the copies and pretend to be the original. Attackers also borrow logos and texts from banks and claim to have bank authorisations.

2.3 Outsourcing

2.3.1 Offshoring

Outsourcing to providers of ICT services in countries with large ICT communities and a lower cost level than Norway, known as offshoring, occurs increasingly. Besides the cost savings involved, many believe that larger, global centres of expertise provide more secure access to expertise and large professional communities, which may enhance the professional level of the delivery.

A knowledge of older technology (Cobol, CICS, IMS, PL/1) may be difficult to maintain in the individual financial institution. It may therefore be advisable to concentrate expertise in international institutions that serve a number of enterprises.

It is important that the institutions ensure that the provider of ICT systems satisfies current Norwegian rules and regulations and best practice.

Cost savings and access to expertise are important factors when institutions consider outsourcing and offshoring. An institution will normally consider its own situation independently of other institutions in the same sector. The societal risk that arises when operating systems for financial services are moved outside the country is a factor that the individual institution probably does not take into account as a basis for its own decisions, but to which weight must be attached in a societal risk assessment.

2.3.2 Cloud computing

The concept of "cloud computing" is often used in reference to deliveries of services from the internet, such as systems for external data storage. These services are a variant of outsourcing.

In cloud computing services, computers and software (IT resources) are shared by the users in question. The IT resources represent a network that stores large quantities of data on a large number of servers.

Cloud services have not previously been well adapted to the financial sector. The following services were launched in 2012.

- NASDAQ OMX Financial cloud
- SAP's cloud-based corporate-to-bank connectivity

If customer and account data are stored in the cloud and banking services are provided as cloud services that are accessible by means of mobile phones, there will no longer be a need

to distribute services in the same way as today. EFTPOS payment terminals and cards may become redundant if mobile phones are used to access customer and account information stored in the cloud. And users can manage with one ID, as compared to the current situation where a user has to juggle many IDs: one or more internet bank IDs, several cards and codes, several VISA/MC secure codes. This will simplify administration and minimise the equipment involved, which will reduce the need for maintenance and hence the risk of error. The cloud is always available.

On the other hand, "Cloud Customers" may become a Single Point of Compromise; in other words, an attacker who steals a user's ID can do a great deal of harm to the user.

Cloud storage can improve operating stability and redundancy. As an example in the Google Apps data are replicated over a number of systems, so that no system is a "single point of failure". The data of each user are replicated to at least two data centres, both of which can serve the user.

At the same time there is a lack of rules and equivalent bodies of agreements for the use of cross-border cloud services, so that resolving conflicts between service provider and customer can be a challenge. There is also a lack of methods to help customers select a provider, given the more pronounced risk associated with using cloud storage.

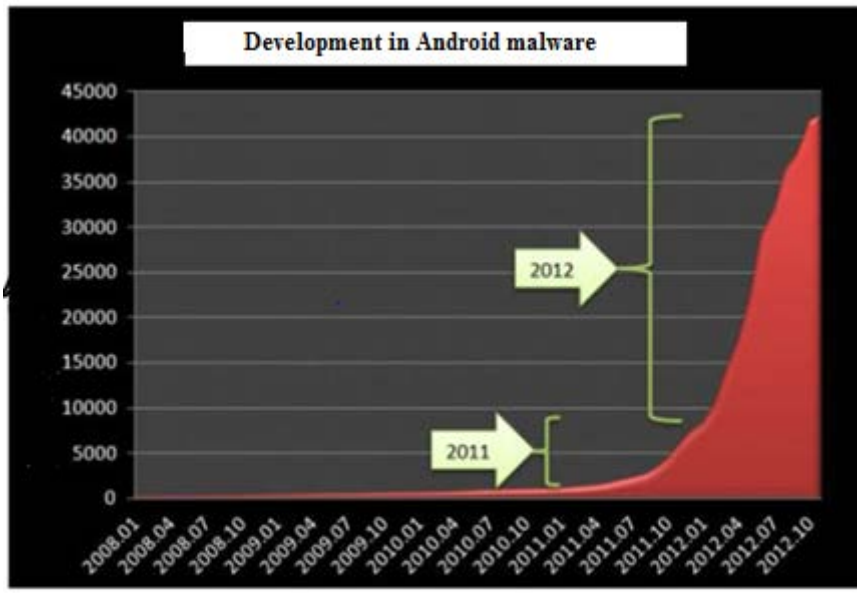
2.4 Developments in payment service systems

2.4.1 Online banking on mobile devices

An increasing number of services are being offered on mobile devices. In Norway, BankID app, Nettbank app and mobilbank app ("mCash") have all been developed recently.

The risks associated with these mobile services are in some respects the same as for banking via a personal computer. However, there is a risk of "mobile malware" associated with mobile services which can be illustrated as follows:

Chart 1: Android malware, assumed development



Source: ZDNet

2.4.2 Use of BankID

BankID, which is banks' shared system for the authentication and electronic signature of bank customers, has now been approved as an electronic ID by the Norwegian authorities. In due course it should be possible to use BankID to log on to about 270 public services.

BankID on personal computers is based on Java software from Oracle. Java is a general development platform for a broad range of equipment and purposes. Recently, a substantial loophole was discovered in Java's security. NorCERT and a number of banks recommended that their customers de-install Java. At the same time, a number of major banks in Norway require that BankID be used. These online banks will therefore be closed to customers who de-install Java. This illustrates how vulnerable the payment system can be. The banks are working actively to make BankID more robust to these threats.

In addition to banking and public services, BankID can be used for a number of other larger and smaller merchants[1]. If users come to use BankID very extensively, they may become less critical about disclosing their log-on codes (national identity number, single-use codes and permanent password) on the internet. Increased used of BankID may increase the risk of users being duped into divulging their codes to someone who unlawfully poses as a BankID merchant.

2.4.3 More sophisticated and aggressive Trojans

Malicious codes (Trojans) have become more sophisticated. The code analyses the customer's computer, finds weaknesses, downloads appropriate malware, monitors the customer's activity and acquires log-on codes or introduces false transactions while the rightful user is logged on. There are databases with an overview of customers who lend out their accounts (mules) as an intermediary for stolen assets. These accounts are retrieved when the attack takes place.

[1] https://www.bankid.no/Dette-er-BankID/Her-kan-du-benytte-BankID/

2.4.4 DDoS

DDoS (Distributed Denial of Service) attacks generate transactions (traffic volume) to a website to "paralyse" the site in relation to other traffic. In 2012 there was a pronounced increase in DDoS attacks against central financial institutions. This is consistent with international trends.

Analyses of DDoS in Norway have not determined whether the objective has been vandalism, testing, camouflage of hacking or shutting down a competitor. The institutions that were subjected to the attacks have taken effective action, in collaboration with NorCERT and Internet Service Providers (ISPs).

2.4.5 Infrastructural weaknesses

Increased demands concerning availability and integration of systems from different providers make heavy demands on networks in terms of quality and availability.

The networks are divided into zones and separated by means of firewalls. The firewall is crucial. Firewall failure may have major negative consequences for many users. At the same time, the number of services and links is growing, which makes maintenance of firewalls more challenging.

2.4.6 Need to modernise core systems

Many of the core systems in the Norwegian financial sector are 20-30 years old. They date from a time when there were few services and few distribution channels. New services have to a large extent been programmed and superimposed on these core systems.

When new services and channels are constantly being established, there is a need to develop solutions where similar functions can be re-used. A report, for example, will typically use functions in a layer that contains various queries (SQL queries), on the database, in a layer that contains database schemas, in a layer with database queries, in a layer with report formatting and in a layer with report presentation. The layers are "sewn together" by means of standardised calls on the layer above or below. The functions in the layers can be copied and used as a template for a similar function in the same layer. Testing can be limited to testing in relation to the layer above and below, as opposed to the situation when there is no planned architecture for solutions and solutions are all separate.

Many banks face challenges related to old architecture. The result is greater complexity with consequent errors and disrupted operations.

Not only is the old architecture complex to maintain; knowledge of the old systems is dwindling rapidly.

2.4.7 Integration

In recent years, Finanstilsynet has been concerned with the risk associated with subdividing of internet service functions from the time a user enters a transaction until final settlement in the bank. In 2012, there was an increase in automated services, which have become integrated with other services, thereby increasing the risk of error.

A network contains a large number of servers and functions. Simple maintenance and stable operations are contingent on all users calling on the same version of a function. There are a number of integration servers for this purpose. The integration system may introduce security loopholes when commands and data are converted from one system to another. An example of this is encryption. Because an integration system converts and passes on orders for information and commands, any encryption has to be terminated in the integration server and then reapplied in the next stage of the integration and communication. An example is conversion from the mobile network to the bank network in connection with mobile banking.

The integration server itself may have weaknesses. As a rule, it also contains a large number of encryption keys, log-on codes and passwords which an intruder can use to attack everything from internal systems to integrated cloud services. If a server is not protected, the attacker may inject messages into the integration system and take control of the target system from within. This is the way in which the DigiNotar certificate authority was compromised.

The challenges of getting an integration server to function as intended may lead to ICT technicians and administrators failing to use the built-in security functions in these products. Moreover, integration systems are seldom perceived as critical to operations; they are regarded more as auxiliary tools, which may lead to security loopholes being overlooked.

2.4.8 Weaknesses in payment cards with chip

A research team consisting of Mike Bond, Steven J. Murdoch, Ross Anderson et al.[2] have discovered a general weakness associated with the generating of security numbers for card payments. Malware is used to phish for transaction information that forms the basis for calculating an authentication code. This information, together with card information and PIN, is sufficient to permit the performance of new transactions that look authentic and also appear to have come from the original payment card with chip. Finanstilsynet is not aware that any such weakness has yet been exploited in the Norwegian payment card market.

2.5 Regulatory developments

Changes in rules and regulations may create a need to make changes in existing IT systems, IT operating set-ups, procedures and supervisory arrangements. These changes may represent an operational risk. The following changes in Norwegian rules have a bearing on work relating to the risk associated with automated financial services.

- The Act relating to business sector contingency measures[3] entered into force on 1 January 2012. The Act regulates collaboration on measures in the event of serious interruptions.
- The Consumer Ombudsman has been of the opinion that telecommunications operators must assume greater responsibility. The Ombudsman[4] wants two contracts for the use of mobile telephones: one for communication and one for payment, which also presupposes authorisation by Finanstilsynet.
- One case concerning cloud storage of e-mails for a Norwegian municipality has provided valuable insight into and explanations concerning the terms and conditions

[2] http://www.cl.cam.ac.uk/~sjm217/papers/ches12preplay.pdf
[3] http://www.lovdata.no/all/hl-20111216-065.html#map001
[4] http://www.forbrukerombudet.no/2012/04/11042228.0

for cloud storage from the point of view of protection of privacy[5]. The Norwegian Data Protection Authority points to the requirement that a risk assessment must be made; see section 13 of the Norwegian Personal Data Act and section 2-4 of the Personal Data Regulations. Agreements relating to data processor's access, security copying, security audits, access protection (encryption), jurisdiction, data erasure and termination are also discussed.

- In June 2012, the Basel Committee published revised guidelines to be used by supervisory authorities to evaluate internal audit functions in banks[6]. The guidelines describe principles for internal audit of banks.
- The European Commission has drafted a new personal data protection regulation[7]. The regulation strengthens the right of private individuals to information as to which data are stored and how they are processed.

2.6 International developments

2.6.1 General initiatives

There is ongoing work in the EU to establish best practice principles for electronic financial services. The following were highlights of activity in 2012:

The European Commission issued a green paper entitled "Towards an Integrated European market for Card, Internet and Mobile Payments"[8]. The report contains proposals for integration of European card infrastructure.

It issues recommendations for a future integrated European card infrastructure. The question of charges is also discussed. Charges must reflect costs and thereby contribute to effective solutions. Customers must be informed about the costs of loyalty programmes and any other customer programmes. The passing on to customers of merchants' costs associated with payment instruments (surcharging) shall cover costs and not be a source of income. Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights[9], which is to be integrated into national legislation by 13 June 2014, will bring excessive surcharging to an end.

The European Payment Council (EPC) recommends that a harmonised certification process for cards and terminals be introduced, and that an approval scheme be developed for the Single Euro Payments Area (SEPA) Cards Standardisation Volume - Book of Requirements[10].

For processing of transactions, the EPC standard ISO 20022 XML is recommended, the same standard that is used by SEPA credit/SEPA direct debits. It is recommended that a common protocol be defined for authorisation and netting, and that a technical interoperability architecture should be developed.

[5] http://www.datatilsynet.no/Global/05_vedtak_saker/2012/11-00593-18%20Avslutning%20av%20sak%20-%20Ny%20e-postl%C3%B8sning%20i%20Narvik%20Kommune%20-%20Google%20Apps.pdf
[6] http://www.bis.org/publ/bcbs223.pdf
[7] http://ec.europa.eu/justice/data-protection/index_en.htm.
[8] http://www.ecb.int/paym/sepa/pdf/2012-03-23_Eurosystem_reaction_to_EC_Green_Paper.pdf
[9] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:304:0064:0088:EN:PDF
[10] http://www.europeanpaymentscouncil.eu/knowledge_bank_detail.cfm?documents_id=560

Harmonised rules, conditions and specifications for internet and mobile payments are also discussed, and reference is made to the EPC's ongoing standardisation process for payments over the internet. Standardised competitive conditions, legal frameworks and security requirements are high priority assignments, on which work is in progress. It is proposed that ISO 20022 XML be used for modern payment systems (internet and mobile) and also other solutions (e-invoicing). Interoperability is encouraged for existing solutions, i.e. exchange of guaranteed payments between systems, based on open standards such as those used in SEPA, (such as ISO 20022 XML, IBAN and BIC).

For the implementation status of all three types of SEPA payments, reference is made to the Seventh SEPA Progress Report[11].

2.6.2 Cloud services

Cloud data processing comes about with the aid of shared IT resources (networks, servers, storage, applications and services), which are allocated as the need arises. Customers pay for use – fixed costs no longer apply. Small and medium-sized enterprises (SME) can thereby gain access to ICT of higher quality than many of them would manage alone. Cloud and mobile units complement one another. The limited storage capacity and functionality of mobile devices is compensated for by unlimited storage and a wealth of cloud functionality. The mobile sector, for its part, ensures a broad user interface with the cloud services.

The European Commission has studied the potential for cloud services in Europe[12], and the EU commissioner for protection of privacy, the European Data Protection Supervisor (EDPS), has issued a statement on the subject[13]. The report points out challenges associated with

- securing and protection of personal data
- control and operations in an infrastructure that is constantly changing
- responsibility and control in a cloud consisting of many providers of services
- data that are often moved around and are therefore exposed

In 2012, Opinion 05/2012 on Cloud Computing[14] was published by the independent EU advisory body Data Protection Working Party. Among the subjects considered were challenges associated with sharing and delimitation of resources, supervision in the cloud, data transport, and storage outside the EEA.

In 2011, the PCI DSS Virtualization Guidelines Information Supplement[15] was issued. Merchants and service providers receive guidance on compliance with PCI/DSS in virtual environments. Attention is drawn to the increased risk introduced by the hypervisor[16] and risk associated with virtual ICT resources generally. In a virtual environment, new resources are constantly being added, while others are being removed. The challenges to supervision that arise in this connection are discussed. The proposal queries whether today's surveillance systems are sufficiently developed to handle the challenges posed by virtual environments.

[11] http://www.ecb.int/pub/pdf/other/singleeuropaymentsarea201010en.pdf
[12] http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf
[13] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf
[14] It is temptingly simple today to copy pictures, text and websites. Attackers use the copies and pretend to be the original.
[15] https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf
[16] Hypervisor: program that controls the resources in the virtualised environment.

2.6.3 Security for internet payments

The European forum for payment security, SecuRe Pay, is a voluntary forum consisting of supervisory and surveillance bodies. SecuRe Pay is now completing its best practice recommendations, based on the Seventh SEPA Progress Report, for security of payment systems over the internet where transfers with creditcards are used[17]. Some of the most important recommendations are:

- Payment Service Providers (PSPs) should have central monitoring and follow-up of security-related incidents and customer complaints.
- PSPs should strip all superfluous functions from servers. Log analysis is required. The security of systems that are in production should be reviewed when new threats arise. The systems should be re-tested in light of new threats.
- Transactions shall be logged and time-stamped. Parameter changes and changes in log files must be traceable.
- E-merchants should support strong authentication by card issuers. All payment systems should encourage strong authentication by transferring responsibility from the merchant to the issuer. Distributed software (applications or applets) should be digitally signed.
- Real-time surveillance and control are encouraged, including checks against blacklists and lists of blocked accounts, and checks of abnormal behaviour patterns. PSPs should urge merchants not to store card data, or alternatively to ensure that they are adequately protected. The card companies' own requirements regarding protection of card data (the Payment Card Industry requirements) will also apply here. PSPs shall provide customers with a secured communication channel, including informing the customer of the procedure for reporting suspicious incidents or non-authorised charges.
- PSPs shall offer customers risk-limiting measures and an alert service. Before start-up, PSP and customer must be agreed on spending limits for both individual transactions and cumulative amounts, and disabling services. PSP should introduce an alert service based, for example, on telephone or SMS notification, for fraudulent payments. The customer should be able to set geographical restrictions.

2.6.4 Automated securities trading

The European Securities and Markets Authority (ESMA) has issued "Guidelines on systems and controls in an automated trading environment for trading platforms, investment firms and competent authorities"[18]. The areas discussed are capacity, continuity, testing, logging and surveillance, security, staffing, management and monitoring and access control.

Functions for deleting orders, excluding members, preventing flooding of order books, controlling access, suspending trading and reporting to the supervisory authorities are also discussed. Examples are also given of market behaviour that points to market manipulation, and which must be kept under surveillance and reported.

[17] http://www.ecb.int/pub/pdf/other/recommendationsforthesecurityofinternetpaymentsen.pdf
[18] http://www.esma.europa.eu/system/files/2011-456_0.pdf

2.7 Concerted measures by the financial industry

Norwegian banks cooperate on a regular basis on security. The work is coordinated by BSK (the Norwegian banks' standardisation authority). The results of incidents, surveillance, analyses and statistics are shared and action decided upon.

Work is in progress to establish a Financial Computer Emergency Response Team (FinansCert) in Norway, to supplement the current voluntary collaboration on surveillance and response to electronic attacks.

The Nordic company Nets Norway AS (Nets) operates a common infrastructure for banks. In 2012, automated controls and analyses of BankID traffic were further developed by the banks through Nets with a view to detecting attacks on both the system and the individual user. The analyses take place in real time, i.e. while the user is logged on, and the intention is that unauthorised use should be stopped before cash transfers take place.

3 Payment service systems

3.1 General information on payment systems

Payment systems are essential to all economic activity. All trading in commercial or financial products culminates in an agreed monetary settlement. In Norway, payment systems are governed by laws and regulations, and through the financial industry's self-regulatory system administered by Finance Norway (FNO).

A payment system is defined as a system based on common rules for clearing, settling and transferring payments between two parties to a financial transaction. A legal distinction is made between an interbank system (transactions between banks) and payment service transactions between customers (retail and corporate) and banks. Payment service systems have been significantly improved by technological advances in recent years, with focus on cost-effective operations, user-friendliness and security.

Electronic payment systems have in practice taken over all transfers of payment. Only an entirely marginal percentage of systems are based on the use of paper forms. Retail customers' use of online banking services accounts for 66 per cent of the number of online bank transactions, while corporate customers' use accounts for 34 per cent. Nonetheless, corporate customers account for over 80 per cent of the value (amount) of the transactions, while retail customers account for close to 20 per cent.

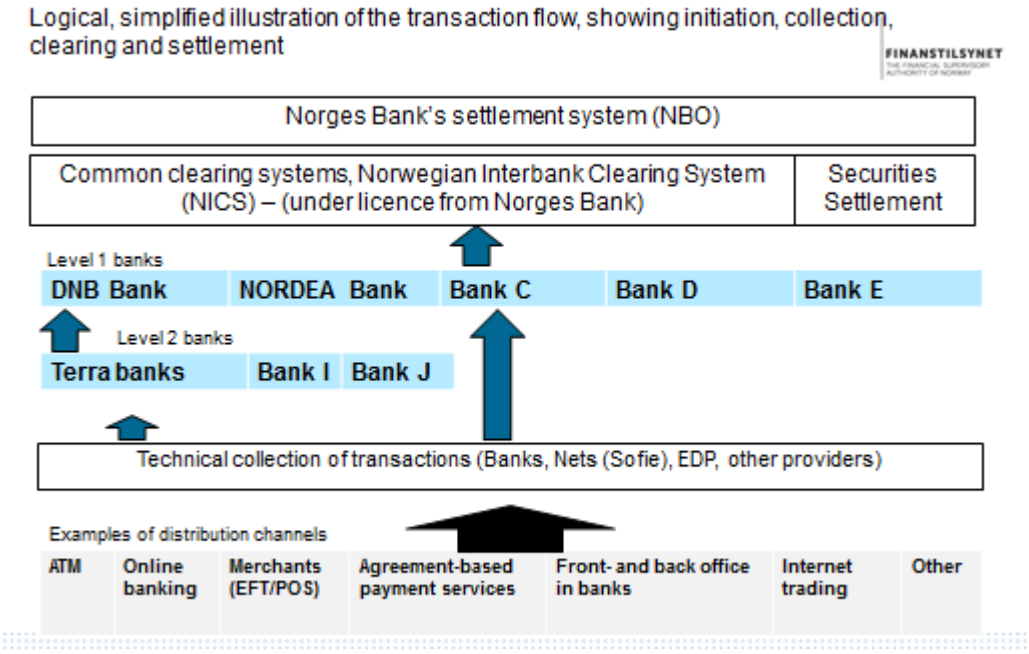
As regards card payments, BankAxept accounts for over 90 per cent of the retail market in terms of value. Norway is a world leader in the use of payment cards.

A large proportion of the electronic infrastructure used by payment systems is outsourced to ICT service providers, but financial institutions' liability for the operations remains unchanged.

Norges Bank's *Annual Report on Payment Systems 2012* contains further information and statistical data on payment systems.

The chart below provides an overview of the transaction flow in the payment system. At the bottom of the chart, there is an illustration of different payment services initiated by customers. Settlement for trades in financial instruments takes place in the securities settlement system (VPO), which is shown second from the top in the chart. The VPO covers the transfer of securities between accounts in the securities register and the transfer of money between buyer and seller. The VPO ensures that no financial instruments are transferred unless payment has been made and vice versa.

Chart 2: Transaction flow



3.2 Management and control of payment systems

Payment systems are a fundamental part of banking services, and are now almost exclusively based on digital solutions. Corporate customers are linked to their banks electronically and information from the bank is used directly in the company's own systems. Efficient liquidity management requires well-functioning, accessible payment and account systems. A coordinated payment system, of the type that Norway has, is contingent on the use of common infrastructure that supports the payment services and provides customers with seamless services. The banks develop their own separate solutions which are based on the common infrastructure and shared solutions. This makes it possible to effectuate payment, clearing and settlement in an integrated operation between a payer in Bank A and a payee in Bank B. This applies even if the payee and Bank B are outside Norway.

Institutions may be faced with difficult decisions in balancing considerations in their routine payment system operations. Current systems must be maintained while new services are developed on the basis of new technology. The new services must be integrated into the existing range of services. Services must be both easy to use and secure. The systems must also be robust in order to withstand increasingly sophisticated criminal attacks.

Clearing, settlement and solutions that support international payments have been relatively stable in operation, and so far have been little exposed to criminal attack. It is primarily customer payment services that are subject to criminal attacks and serious incidents.

It is important to ensure that all elements and participants in the transaction chain between payer and payee are covered in the management of operational risk. It is also important to ensure that IT providers and any subcontractors have the requisite expertise and time to be able to manage and control the running of their own operations.

Some financial institutions find it a challenge to maintain sufficient control of this aspect. A framework must be established for management and control of operations, which includes establishing procedures for important functions. Control systems must be put in place to ensure compliance with rules and with the established level of quality. Regular risk assessments must be carried out to ensure that measures are initiated to prevent criminal attacks and avert serious incidents. The establishment of a preparedness system and exercises in its use are also necessary to be able to act effectively when incidents nevertheless occur. Ensuring that such measures are in place is a management responsibility.

The Payment Systems Act requires that Finanstilsynet be notified without undue delay of the establishment and operation of payment services. In 2012, Finanstilsynet received 5 notifications, two concerning SWIFT, one concerning the installation of BankID, one concerning BankID on mobile telephones and one concerning cards with RFID technology. The main purpose of this duty of notification is to ensure that the necessary risk assessment has been carried out and that any agreements between the parties concerned are established before a new payment service is utilised. There is reason to assume that changes in payment service systems are underreported, and Finanstilsynet will consider further action to ensure compliance with the notification duty.

3.3 Risk and vulnerability in payment systems

3.3.1 BankID

BankID is used to a growing extent in payment services and has consequently become increasingly important. BankID is used for authentication purposes and for the electronic signing of transactions. When used on a PC, BankID is chiefly based on the Java development kit. In 2012, there were cases where new Java updates caused security holes in the Java code. Consequently, BankID has begun work on finding possible alternatives to the Java-based solution so that individual users of BankID stored by the bank do not need to download Java in order to use BankID.

BankID already has an alternative to the Java-based solution: BankID on mobile telephones. The user's BankID is stored in the mobile phone's SIM card. DNB, Skandiabanken, the Terra banks and Sparebank1 offer this service in collaboration with Telenor, Djuice, Talkmore, Hello Norway or Phonero. With time, more banks and mobile device providers are expected to gradually offer this service.

In November 2012, the Agency for Public Management and eGovernment (Difi) entered into a contract with BankID for the delivery of a high-security electronic ID for public digital services. The fact that the BankID solution is also used outside the financial infrastructure by both the public administration and private non-financial corporations could constitute a risk. The new merchants will not necessarily have the same standards of security and risk management as financial corporations.

3.3.2 Malware

Use of phishing as a method for stealing data has become an extremely common form of attack for the unlawful collection of data. The data are misused, for example in online transactions for which a payment card is used. This form of payment card use is called a "card-not-present" transaction. Misuse often occurs in connection with payment for goods from online stores, particularly in stores that do not require security solutions such as BankID

or 3D-Secure. Trojans are becoming increasingly sophisticated and consequently harder for traditional anti-virus software to detect. Trojans can be spread in several ways, but the two most common methods are by embedding the malware in an e-mail attachment or by inserting the malware in an advertisement or a link, for instance in an online newspaper or a search engine. If the search engine providers do not have good systems for detecting links that contain malware, an infected link can be placed at the top of the list of search results for the most popular search words. When PCs are infected by Trojan malware, this malware can be used in attempted fraud. This applies in particular to online banking fraud when the owner of the PC uses his or her PC to access the bank.

3.3.3 Attacks on EFTPOS terminals and ATMs

Both ATMs and EFTPOS terminals are vulnerable to skimming. Firstly, ATMs are targets of "cash trapping", where banknotes are stolen from customers. We are seeing creative new solutions. Both adhesive strips placed on the cash dispensing slot and fork-like devices inserted in the cash dispenser are used to snare the money. Secondly, both EFTPOS terminals and ATMs are targets for real skimming, where the data on the card's magnetic stripe are read.

So far, there have been no reports of a chip being successfully compromised. However, activity has been observed in the form of "chip-skimming", where an electronic circuit board is installed in the chip reader in an attempt to read the data exchange that takes place between the chip and the receiver.

3.3.4 Mobile telephone solutions

Use of mobile telephone solutions has increased significantly in 2012 and will in all likelihood continue to increase in the next few years. The solutions are user-friendly and new functions are constantly being introduced. The mobile solutions are often divided into two levels of security. A personal password is often sufficient to enable a bank customer to check his account balance and transfer funds from one of his accounts to another. If the customer wishes to pay a bill, he must also enter a single-use code in addition to his password.

There are two types of operating systems that are market leaders in smart telephony: Google's Android and Apple's IOS. It is common knowledge that Apple's operating system offers higher security and that Apple's systems enabling a developer to install an app in Apples App Store are more secure than the solutions that Google has for Google Play. This means that Android smart telephones that download apps from Google Play have far weaker security. The possibility of the telephone being infected with malware when apps are downloaded is therefore greater than in the case of Apple solutions.

Norwegian banks have initiated pilot projects where credit cards have built-in RFID[19] functionality. RFID functionality is relatively well proven technology that is used, for instance, in admission cards. It enables one-way communication between the card and the reader. When the card is held up to the terminal, the payment data are transmitted between the credit card and the terminal.

In parallel with this, pilot projects are being conducted using Near Field Communication (NFC) technology. It has functions similar to those of RFID, but is used in mobile telephones

[19] RFID – Radio Frequency Identification

(smart telephones). In an interaction between NFC and a SIM card with a payment application, a payment terminal that can read RFID can also read NFC signals and execute a payment transaction.

Both technologies can entail the following risks:

- Data transmitted between a card/telephone and a reader can be captured and sensitive information relating to the card can be stored and misused, for instance by cloning a card.
- Data transmitted between a card/telephone and a reader can be captured, changed and retransmitted for processing.

This last risk applies particularly to smart telephones that use the Android operating system. Although there have been few incidents so far involving viruses on mobile telephones, this problem is predicted to increase in scope. NFC technology enables users to store bank account and card data on their smart telephones.

In view of the growing use of mobile telephones as a payment channel, it is important that banks require the same standard of security for mobile solutions as for traditional online banking solutions. Mobile solutions are increasingly exposed to the same risks as traditional online banks. It is therefore important that the solutions, such as the use of SSL certificates, offer the same strong encryption in mobile solutions as at work stations.

3.3.5 Concentration risk

More and more financial services are being linked together and share technical resources. An error in one of the services can cause one or more of the other services to also fail.

Nets Norway AS (Nets) carries out services for banks that can be described as the hub of the payment service infrastructure. Payment services like BankAxept, BankID and the NICS[20] clearing system are all solutions that are administered and operated by Nets. The BankAxept card is the most commonly used card in Norway, and every month in 2012 this card was used to pay for goods and services averaging over NOK 40 billion in value. According to www.bankaxept.no, over 8 out of 10 card payments in Norway are made using BankAxept. According to Norges Bank's Annual Report on Payment Services 2011, cash as a share of the value of means of payment available to the public was approximately 6 per cent, which is a 50 per cent reduction in the past decade.

Most of the banks use the IT provider Evry ASA (Evry) to perform a number of tasks of varying importance. Consequently, if a service becomes inaccessible, the problem often affects more than one bank. One of the services where several banks use the same solution is the engine in the RBS bill payment system. This system must be functioning in order for bank customers to be able to pay bills. Another example is PIN verification. Due to this type of concentration risk, Evry focuses attention on its business continuity and disaster recovery plans. In 2012, some of the IT services that Evry delivers to the finance sector again suffered serious errors and/or deficiencies that rendered services inaccessible to banks and bank customers.

[20] NICS – Norwegian Interbank Clearing System

3.4 Overview of losses related to payment services

3.4.1 Losses in Norway

The tables below show losses in Norway due to payment card and online banking fraud in the last two years. The figures were obtained by Finance Norway and BSK (the Norwegian banks' standardisation office) in collaboration with Finanstilsynet.

Table 1: Losses related to use of payment cards (figures in NOK 1,000s)

Type of payment card fraud	2011	2012
Misuse of card information, card not present (CNP) (internet transaction)	24 190	35 701
Stolen card information (including skimming), misused with counterfeit cards in Norway	468	2 308
Stolen card information (including skimming), misused with counterfeit cards outside Norway	57 340	55 869
Original cards lost or stolen, misused with PIN in Norway	32 224	28 128
Original cards lost or stolen, misused with PIN outside Norway	7 008	8 544
Original cards lost or stolen, misused without PIN	4 488	4 603
TOTAL	**125 718**	**135 153**

Source: Finanstilsynet

Payment card losses increased in 2012, primarily due to an increase in card-not-present (CNP) fraud. Such fraud occurs in connection with purchases entailing the use of card data online (primarily), by telephone or by e-mail. Fraud accounted for around 0.017 per cent of the total value of payment card transactions in Norway in 2012. Relatively speaking, this is somewhat lower than elsewhere in Europe. The trend towards a rise in CNP fraud is on a par with the rest of Europe.

Table 2: Losses related to use of online banking (figures in NOK 1,000s)

Type of online banking fraud	2011	2012
Attacks using malware on customer's PC (Trojans)	664	5 064
Attacks that exploit vulnerabilities in online banking applications (hacking)	0	0
Lost/stolen security device	3 321	3 367
TOTAL	**3 985**	**8 431**

Source: Finanstilsynet

Losses related to online banking increased in 2012 due to the increase in attacks by international criminal groups involving the use of Trojans. In terms of amounts, however, the losses are still small. To obtain an accurate picture of the level of fraud, since the second half of 2012 banks have been reporting two other parameters in addition to loss:

- Fraudulent transactions recorded in the online bank with a valid account number and an amount, but averted before they could be executed.
- The number of customers whose computer has been discovered by the bank to be infected with an active online banking Trojan.

These figures indicate that the potential losses are significantly higher. While Norway has seen a substantial increase in the number of attacks in 2012, as have countries like Belgium and the Netherlands, other countries, such as the UK, are experiencing a decline in the number of attacks.

3.4.2 Losses in other European countries

The following comments apply to the figures for losses elsewhere in Europe. The information has been obtained from reports issued by the European ATM Security Team (EAST)[21], Financial Fraud Action UK[22], Observatoire de la Sécurité des Cartes de Paiement[23] in France and the European Central Bank (ECB)[24].

Card-related losses have fallen in most European countries since the chip was introduced. A typical example of this trend can be found in the UK, where there has been a steady decline in losses since 2008. Fraud accounted for 0.061 per cent of total transaction amounts in 2011. The decrease is greatest for losses arising from the use of counterfeit cards. The percentage of CNP losses in relation to total losses has increased every year.

As a result of the introduction of the chip-and-PIN system, counterfeit card fraud has declined all over Europe. Fewer and fewer countries allow the use of a magnetic stripe. Regional card blocking (geo-blocking) to prevent use of cards in such areas as the USA or Central America has further reduced losses. Some countries have introduced strict regulation of geo-blocking. One example is Belgium, which has made geo-blocking mandatory. This has reduced losses arising from the use of counterfeit cards by over 95 per cent.

Together with up-to-date anti-skimming equipment, geo-blocking has also led to a substantial decrease in ATM skimming.

The smallest decline is seen in CNP losses, arising from payments made by e-mail, telephone or the Internet. Neither the card nor the card user is present when the fraudulent act occurs and it can be difficult to detect. Measures to combat such fraud include password protection such as Verified by Visa, monitoring and billing address verification.

There is a slight increase in misuse of original cards. This may be because the production of counterfeit cards is no longer as profitable. As a result, some of the fraud is carried out using more manual methods.

Online banking losses vary significantly from one country to another. In 2012, there was a substantial increase in such losses in Belgium[25] and the Netherlands[26]. In the UK, losses have declined in recent years. The magnitude of the losses does not necessarily reflect the intensity of the attacks. Efforts to combat this problem are mitigating the size of the losses; see loss statistics for Norway in 2012.

[21] https://www.european-atm-security.eu/Press%20and%20Media/
[22] Financial Fraud Action UK – Fraud The Facts 2012: http://www.financialfraudaction.org.uk/downloads.asp?genre=consumer
[23] Report for 2011: http://www.banque-france.fr/observatoire/rap_act_fr_11.htm
[24] European Central Bank (ECB) – Report on card fraud July 2012 : http://www.ecb.int/pub/pdf/other/cardfraudreport201207en.pdf
[25] http://www.febelfin.be/nl/veilig-internetbankieren-enkele-tips
[26] http://www.nvb.nl/veelgestelde-vragen/1351/hoe-hoog-is-de-schade-door-fraude-met-internetbankieren.html

4 Findings and observations

Finanstilsynet's observations are based on IT inspections, reported incidents, year-end RAV interviews (see 4.2), meetings with institutions and service providers and special projects. Another important source of information was the banks' replies to Circular 20/2011 following the disruption of service during Easter 2011.

4.1 Some findings from IT inspections in 2012

In 2012, Finanstilsynet decided to conduct thematic inspections in selected areas of ICT activity, resulting in fewer, but more extensive inspections. The topics chosen were disaster recovery and contingency systems, electronic payment services, and governance of ICT infrastructure.

4.1.1 Business continuity and disaster recovery plans

Business continuity and disaster recovery plans necessitate close cooperation between the institution and service providers that administer and/or run the systems. The plans must cover a variety of scenarios in which several levels may be affected simultaneously. Thorough risk assessments and action plans are essential.

End-to-end testing of business continuity and disaster recovery plans requires that the institution concerned and its service providers carry out joint testing and exercises. These matters must be stipulated in outsourcing contracts. Putting this testing in place later on may prove to be costly and this could be an incentive to postpone the matter or give it lower priority.

Institutions often refer to tests of business continuity plans for individual systems and disaster scenarios that affect operations locally at the institutions' head office. There seems to be a tacit agreement that contingency testing is left to the outsourcing partner. The institutions show a lack of engagement in this connection. The testing is conducted at each individual level of the chain, for scenarios that have a local impact, and there is no test that satisfactorily covers the interoperability aspect.

On-site inspections have also revealed inadequate documentation of prerequisites and system interdependencies. This makes it difficult to determine priorities in a crisis.

It is the banks' responsibility to ensure that plans and tests are satisfactory, and that training is provided. Some institutions have no training activities other than the technical test.

4.1.2 Growing risk related to old, complex core systems

Most banks utilise core systems that are old, and they often use technology that cannot easily be adapted to meet today's communications and operations/maintenance requirements. New functions and systems are now available and have been linked to the core systems in various ways. New user interfaces have been developed based on new technology and superimposed on the old ones. Bank systems have therefore become highly complex and, to some extent, convoluted. Errors can easily arise when acute problems need to be solved in a great hurry.

There are several reasons for this situation. Banks are often organised on the basis of customer segments, and systems are developed along the same divisions. Overall solutions are not given sufficient priority. For many banks, especially the smaller ones, the way through outsourcing to service provider is long. The distance between the systems and the persons responsible for them in the banks is great, and attention is focused on operations and costs, in addition to new functions. Consequently, the modernisation of systems and technology is paid little attention by governing and funding bodies and is often not given high priority.

Several banks now consider the risk related to the old, complex core systems to be increasing, and some are finding it difficult to recruit personnel with expertise in the technology that has been used. There is a growing recognition that major investments are now required to renew and rationalise the core systems.

4.1.3 Follow-up of identified risks

Local inspections have revealed that the follow-up of risks and vulnerabilities that have already been identified is inadequate. Initially, the institution does a satisfactory job of assessing risk, analysing incidents to uncover their causes and prevent them from reoccurring, and testing business continuity and disaster recovery plans. This process culminates in specific measures and action plans.

Activities specifically designed to mitigate identified risks are often postponed. Postponement can be due to technical problems, cost considerations, problems with service providers, time pressure, freeze periods, etc. It has been seen that such postponement can result in the pulverisation of responsibility and lack of clarity as to who is responsible for implementing the measures. Measures can be eliminated or forgotten. Some serious incidents in the past few years have been caused by the failure of components in which a vulnerability had already been identified. The reporting and follow-up of such matters must therefore be improved.

4.1.4 Changes made by the service provider

When services are outsourced, the service provider often regards certain changes as “his”, because they are necessary from a technical standpoint. Changes in such areas are therefore not always notified to institutions to enable them to assess the impact on their own critical systems. The institutions are therefore not prepared for the eventuality that problems may arise, and for possible conflicts with other activities at the local level. Nonetheless, Finanstilsynet notes that there has been improvement in this respect in 2012.

4.2 Institutions’ own assessments

In order to gain insight into the financial institutions’ own assessments of their ICT risk, Finanstilsynet conducted dialogues with thirteen financial institutions of various types and sizes in 2012. The dialogues concerned problems and challenges experienced in 2011, and the risks that they anticipate as being the most serious in 2013. Finanstilsynet also wished to obtain an overview of the institutions’ use of cloud computing.

The institutions considered the following to be the greatest problem areas in 2012:

- *External attacks*
  Virtually all institutions report that external attacks, such as Trojan attacks, hacker attacks and DDoS posed a significant challenge in 2012. For banks, such attacks

largely consisted of attempted online banking fraud. The number of attacks or attempted attacks increased substantially in 2012, the methods change rapidly and have required considerable attention and preparedness on the part of the institutions.

- *Disruption of or unstable operations*
  Many of the institutions have found disrupted operations and unstable or slow operations caused by erroneous handling or errors due to the complexity of the infrastructure and network to be a problem. The institutions largely attribute this problem to service provider-related circumstances.

- *Outsourced activities*
  Many institutions have indicated that outsourced activities present challenges, including issues other than the operational problems mentioned above. Institutions have experienced problems in the form of inadequate compliance with SLA agreements, and inadequate delivery by and unsatisfactory collaboration with service providers. Some institutions which have outsourced system development to India (offshoring) have, for instance, found that the provider lacked the necessary expertise and that the quality of deliveries was unsatisfactory.

- *Change management*
  The overall impression is that change management is an area in need of general improvement. This applies both to operational changes and application changes carried out by the institution itself and by the service provider. Most errors occur in connection with a change.

Areas of risk in 2013:
The institutions consider that the areas that caused the most problems in 2012 also constitute the greatest risks in 2013, despite the measures that have been taken:

- *External attacks*
- *Disrupted and unstable operations*
- *Outsourced activities*
- *Change management*

Several institutions also mention the following risks:

- *New platforms and new technology*
  In this connection, special mention is made of the presumed lack of knowledge of the risks related to use of mobile telephones/smart telephones.

- *The expertise and resource situation*
  This applies in particular to expertise and resources relating to older systems and technology, for which fewer and fewer persons have the relevant skills and which are not attractive to newly trained persons.

- *Inadequate disaster recovery plans and verification through testing*
  Some institutions point to the risk that crises may not be handled satisfactorily because disaster recovery plans and/or testing of such plans are inadequate.

Use of cloud computing
Some institutions have begun to use cloud services in a limited area, such as in connection with recruitment and employee performance assessment interviews, but have no plans to make more extensive use of such services. Other institutions do not use such services at all, nor do they have any plans to do so. Several of the institutions assess the risk related to cloud services as uncertain and/or too great.

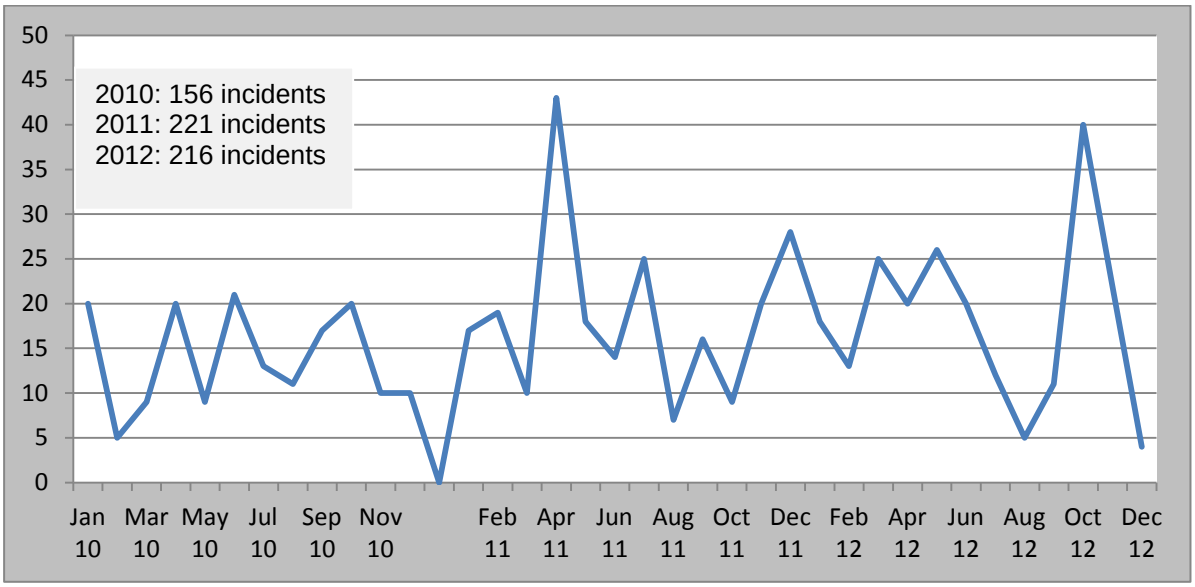
4.3 Incidents reported in 2012

The number of incidents reported in 2012 was at approximately the same level as in 2011. There was a rise in the number of malicious attacks, both Trojan attacks and DDoS attacks. The number of attacks on ATMs also increased.

Some serious operational incidents occurred in 2012.

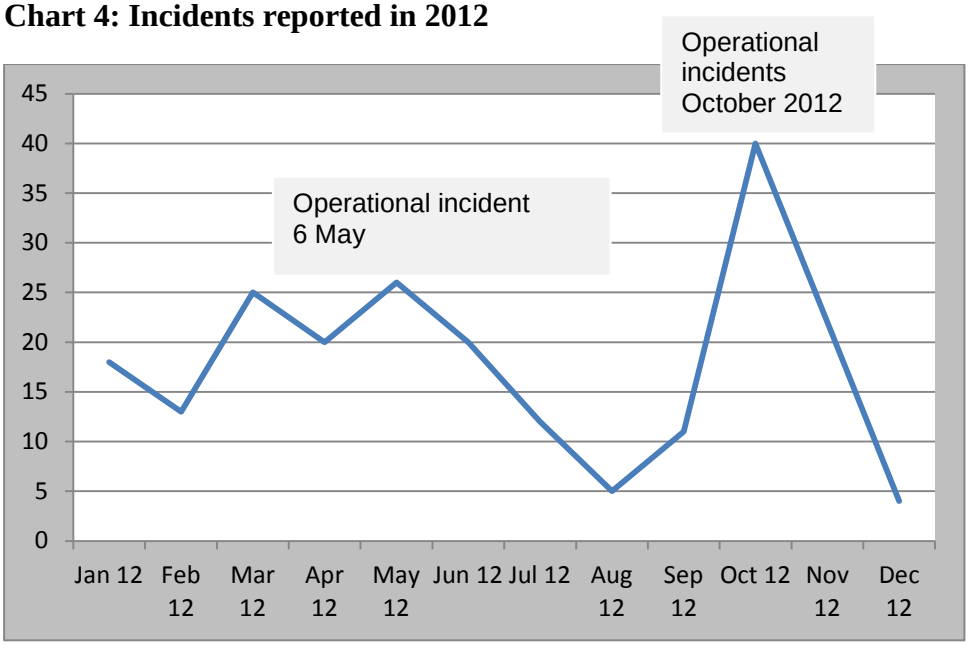
In September, a serious incident took place in the Norwegian Central Securities Depository (VPS) in connection with erroneous registration that led to the unintentional erasure of data.

Chart 3: Number of incidents reported, 2010–2012



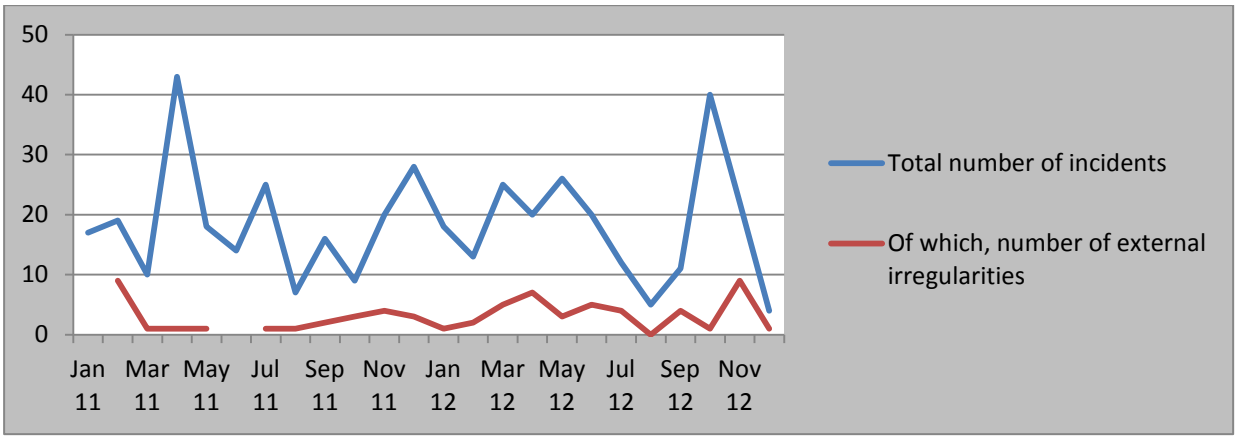
Source: Finanstilsynet

Chart 4: Incidents reported in 2012



Source: Finanstilsynet

Chart 5: Number of reported malicious attacks, 2011–2012



Source: Finanstilsynet

4.3.1 Trojan attacks

The banks reported the occurrence of Trojan attacks throughout 2012. There were attacks by different types of Trojans, beginning with varieties of Zeus and SpyEye and followed by Ice IX and Torpig. The last Trojan has been particularly challenging to handle. It is unpredictable, collects data before it attacks, is difficult to detect and recreate, appears to the customer in different guises and changes in response to every countermeasure that is implemented. Many customers have had their PCs infected. Among other things, a large wave of phishing e-mails in the name of DnB was a source of infection. Nevertheless, losses were low because of the extensive efforts of the banks and their shared partners like BSK and NorCERT.

Most of the account numbers to which the transaction amounts are to be transferred are still located outside Norway, but active efforts are also being made to recruit Norwegian account holders (mules) to make their accounts available. This recruitment is disguised as an ordinary appointment to a post in a small financial institution which carries out payments and where the employee is remunerated with a small percentage of the turnover. In this way, more or less unsuspecting persons are recruited in Norway to act as money mules and thus in fact as receivers of stolen goods by making their account available for a criminal act.

Chart 6: Excerpt from a letter recruiting a "Payment Institution Agent/Money Transfer Agent (= money mule)

PAYMENT INSTITUTION AGENT

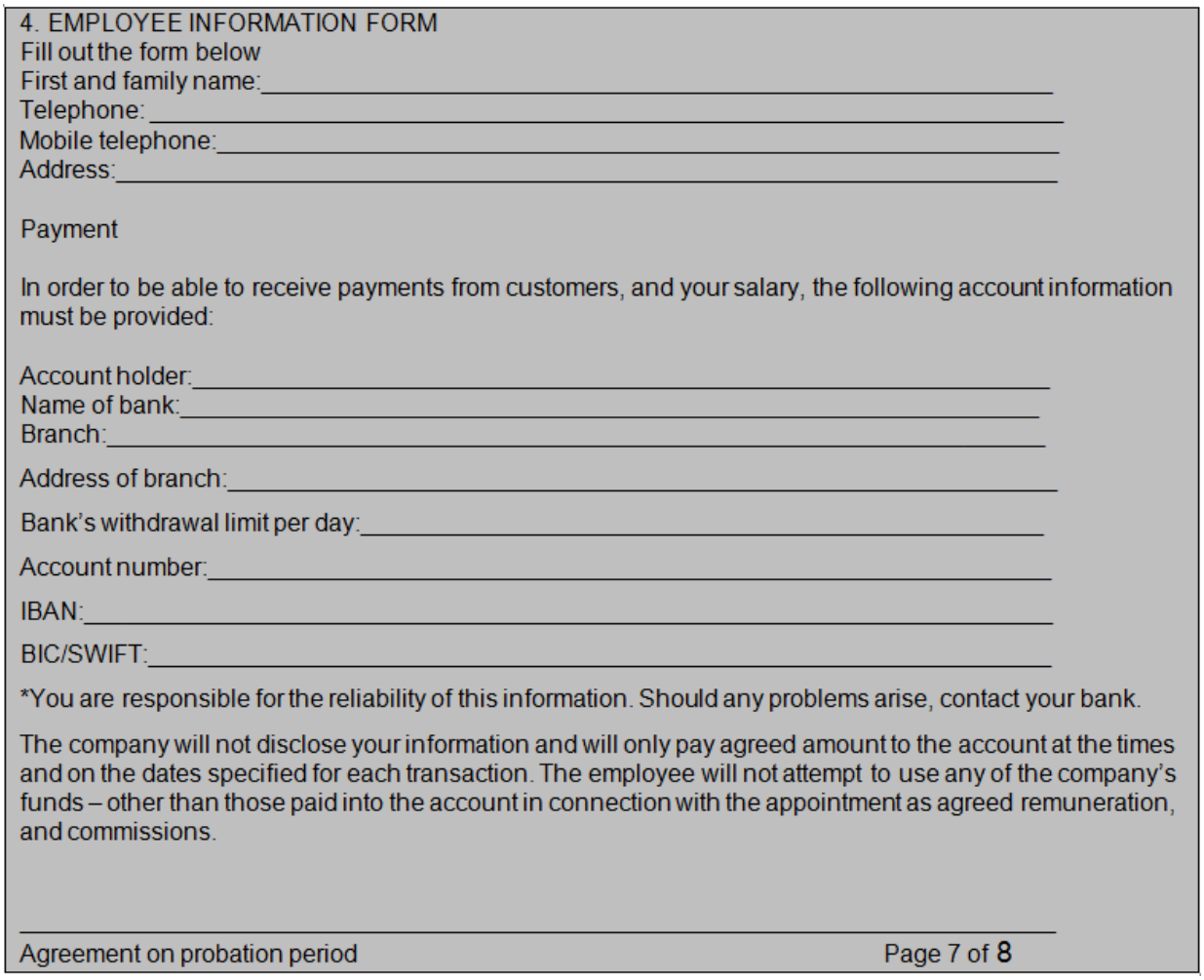
We are looking for people to process payments received from our customers. The company will give the agent detailed instructions that are relevant for the payment process, including the full name of the payer and the amount involved in every single case.

When the funds have been deposited in the employee's account, it is the finance agent's duty to withdraw money and transfer the funds by means of an international bank transfer or by using the international WesternUnion/MoneyGram money transfer systems.

SALARY

During the probation period, we offer a salary of EUR 2000 per month plus a commission of 5% for each payment processed.

Chart 7: Part of the "employment contract" for "Payment Institution Agent" (= money mule), in which the person is asked to fill out information regarding his or her bank account. The language is relatively good, but spelling mistakes and unprofessional style will still be found upon closer examination of the text.



4. EMPLOYEE INFORMATION FORM
Fill out the form below
First and family name:_____
Telephone: _____
Mobile telephone:_____
Address:_____

Payment

In order to be able to receive payments from customers, and your salary, the following account information must be provided:

Account holder:_____
Name of bank:_____
Branch:_____
Address of branch:_____
Bank's withdrawal limit per day:_____
Account number:_____
IBAN:_____
BIC/SWIFT:_____

*You are responsible for the reliability of this information. Should any problems arise, contact your bank.

The company will not disclose your information and will only pay agreed amount to the account at the times and on the dates specified for each transaction. The employee will not attempt to use any of the company's funds – other than those paid into the account in connection with the appointment as agreed remuneration, and commissions.

_____
Agreement on probation period Page 7 of 8

4.3.2 Distributed Denial of Service (DDoS) attacks

From being a virtually non-existent phenomenon in Norway, DDoS attacks on financial institutions increased significantly in 2012. The largest banks, Oslo Børs and ICT service providers have been attacked. The most serious incident was the DDoS attack on Oslo Børs in June 2012. Access to Oslo Børs's website was reduced for one week as a result of an attack that varied in intensity. In the past few years, effective measures to combat DDoS attacks have been developed. Dummy packet traffic can be recognised and filtered in both ISP networks and in the institutions' own systems. The DDoS attacks have therefore had little impact on customer services or operations.

4.3.3 Operational incidents

The number of operational incidents remained at the same level in 2012 as in 2011. After some incidents in March and a more major incident in May, there were few serious incidents until October and the rest of the year when several incidents occurred. There was no single incident as serious as the "2011 Easter incident", but there were a number of incidents that

affected many banks simultaneously. These incidents were caused by several different errors in components of Evry's central shared infrastructure.

After the Easter incident in 2011, Evry launched its "Leave-No-Stone-Unturned" programme to map vulnerabilities in payment channels. In 2012, Evry expanded the programme to cover its central shared infrastructure consisting of networks, servers and mainframe computers.

4.3.4 Attacks on ATMs

Despite the fact that it has become more difficult to use cards with a magnetic stripe, counterfeit card losses are still substantial in Norway. In 2012 there was an increase in attacks on ATMs in Norway. Several methods are used:

- Social manipulation, often of elderly persons. While engaged in dialogue with the ATM, the card owner is distracted and the criminal pulls out the card without the customer noticing
- Cash trap – the money sticks to a device that has been attached to the cash dispensing slot
- True skimming in cases where the anti-skimming device installed on the ATM has not been upgraded

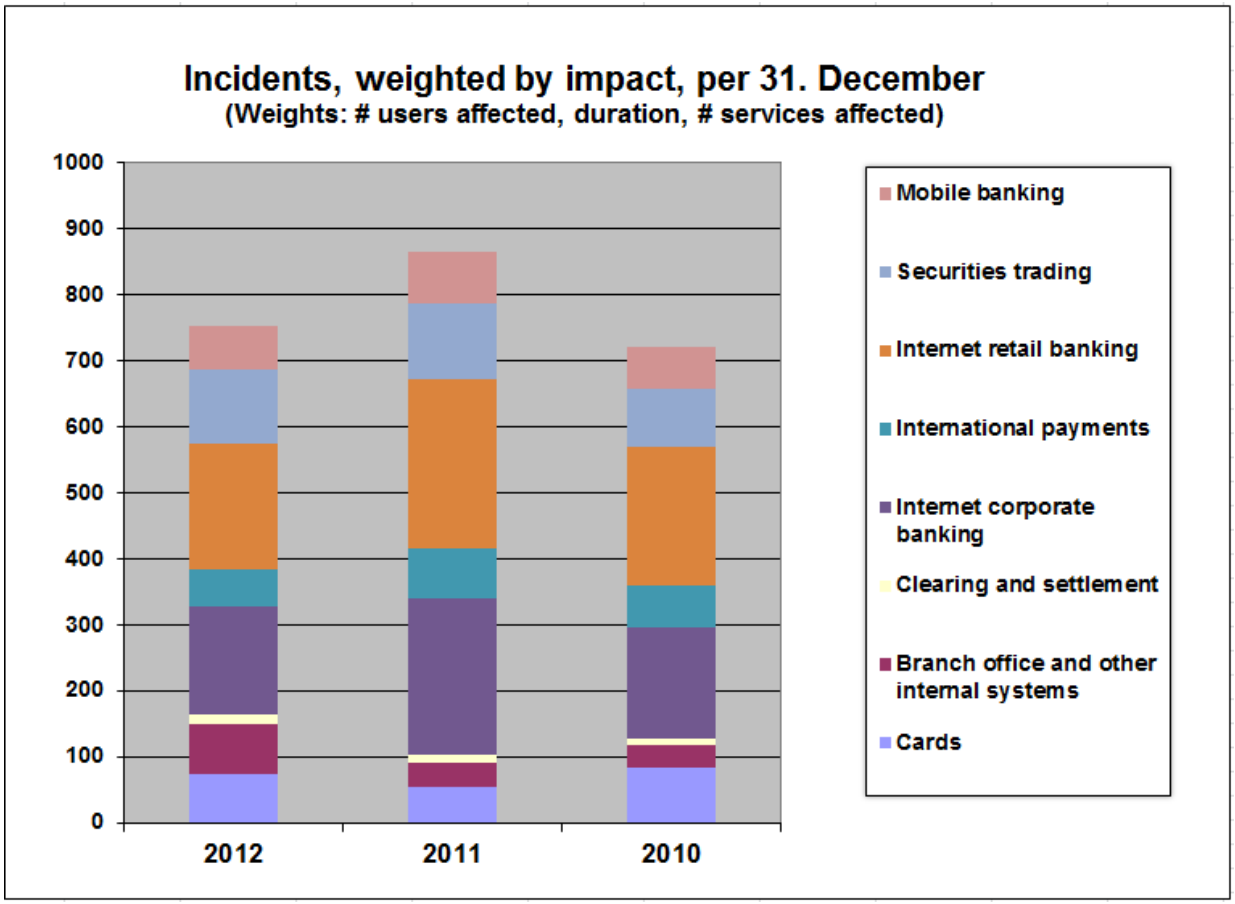
The banks continuously update ATM anti-skimming equipment.

4.3.5 Analysis of incidents

Finanstilsynet often receives reports from several banks about one and the same incident, when the incident has occurred at their common service provider. Nonetheless, it is not the case that all banks are affected in the same way, neither in terms of the type of services or the duration of the interruption of service.

On this basis, Finanstilsynet has analysed the incidents that occurred in 2012. The scope of the incidents has been assessed on the basis of the number of users affected and the duration of the interruption of service. The damage has been assessed in the case of each incident, based on identical criteria. The incidents can therefore be summed up for each year and for each service and compared over time. The vertical axis in Chart 10 expresses a weighted, total assessment of the impact of the incidents, providing an index that reflects the unavailability of bank services.

Chart 8: Incidents weighted by impact



4.4 Results of projects carried out

4.4.1 Critical ICT components

After the card system problems experienced during Easter 2011, Finanstilsynet asked the banks to document critical components in their ICT infrastructure, and to describe their procedures for monitoring service providers' change management and preparedness; see Circular 20/2011 on more stringent requirements for banks in the light of the operational problems during Easter 2011.

The banks and their service providers have prepared relatively detailed descriptions of the critical components, and to varying degrees have carried out a vulnerability analysis of them. Action has been taken where the level of vulnerability was found to be too high. Evry has initiated the "Leave No Stone Unturned" programme, which is aimed, among other things, at improving quality.

Traditionally, the maintenance, handling of errors in and upgrading of systems have to some extent been left up to the service providers. Several banks have now installed their own change management systems which formalise interaction with providers with respect to changes.

Coordinated preparedness has been strengthened in specific terms by the establishment, initiated by Finance Norway, of an interoperability procedure in response to errors and incidents in BankAxept's value chain. The interoperability procedure applies to all service providers and banks. Furthermore, Nets and Evry have entered into a new bilateral agreement on interoperability. Several banks have announced that they will now conduct joint exercises with their service providers.

Most of the banks explicitly confirm their responsibility for their portfolio of systems and that from now on they will monitor their service providers' work more closely.

4.5 Risk areas identified by others

4.5.1 Importance of the mobile network

Mobile telephones have moved up from being the secondary to the primary telecommunications channel, and the mobile network is used increasingly for financial services.

In 2011, Hurricane Dagmar revealed how vulnerable society has become if the mobile network goes down. The extreme weather made it clear that large areas may lose most means of electronic communication if the access networks for mobile telephones suffer extensive damage.

In January 2012, the Norwegian Post and Telecommunications Authority (PT) published the report "Preliminary experiences and proposals for action following Hurricane Dagmar"[27], in which a number of proposals for improvement were presented. PT proposes requiring providers to have back-up power for at least six hours of operation at the great majority of base stations, and will take the initiative to establish a programme to strengthen base station locations that cover particularly important areas. The objective is to secure 1,000 base station locations nation-wide and require providers to safeguard these with batteries and generators for three days of operations.

A further measure proposed by PT is to introduce priority in the mobile networks. Many societal functions today are dependent on mobile communications. In the event of a shortage of network capacity in a crisis or emergency situation, it is important to have arrangements that clearly prioritise functions that are critical for the community.

4.5.2 Test of security level of cloud services

A British survey conducted by BAE Systems[28] resulted in a set of recommendations for those considering outsourcing services to a cloud provider/cloud service provider (see below).

- Check that the cloud service provider has high-end firewall and IDS.
- Check whether the cloud service provider undertakes regular, independent security tests of the operating environment. Make a thorough check of whether the cloud service provider's security model is compatible with the user's own security architecture.

[27] Post- og teletilsynet, rapport nr. 2 2012: "Foreløpige erfaringer og forslag til tiltak etter ekstremværet Dagmar"
[28] http://baesystemsdetica.blogspot.no/2012/10/botcloud-emerging-platform-for-cyber_785.html

- Be aware of possible botCloud attacks. The traffic coming from public Cloud providers should not necessarily be deemed safe.

4.5.3 Findings in the threat report of ENISA

ENISA (The European Network and Information Security Agency) is a network of EU information security experts who draw up guidelines and recommendations for good information security practice. In the autumn of 2012, ENISA published the report "ENISA Threat Landscape"[29], which considers threats to cyber-security and is based on an analysis of over 120 reports and findings from the IT security industry, standardisation bodies, IT security networks and other independent organisations. In addition to ranking threats, the report concludes with a set of recommendations.

Important elements are better end-to-end documentation of the attack scenario, better documentation of the consequences a successful attack may have, and shared terminology. ENISA's threat list is headed by drive-by exploits[30] and Trojans.

[29] http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISAThreatLandscape
[30] In drive-by exploits, users are exposed "in passing" by opening/clicking on links on or in e-mails that initiate the download of malicious code to the user's computer without the user being aware of it.

5 Identified areas of risk

5.1 Management and control

Financial institutions are responsible for all information and communication technology they use in their operations. Finanstilsynet often finds that the institutions regard the providers as responsible. This can lead to inadequate management and control.

Finanstilsynet believes that the rights and obligations of the individual banks associated with coordinated shared systems (BAX, NICS, BankID and others) are not well enough defined. This applies to ownership rights, rights of use, development and administration.

Systems providers are constantly changing; they restructure, sell, merge or move. Institutions are outsourcing a growing number of services. In this situation it is important that the institutions have the freedom to choose a direction other than the one chosen by the provider. This makes it important to have clear right of ownership and use of software, documentation and other intellectual property rights (IPR) that are included in the solution.

5.2 Attacks on internet-based systems

The institutions report that they regard criminal attacks as a major challenge and are increasing their efforts to keep the attacks under control. Trojan codes are sophisticated, often composed of several modules so that one and the same Trojan can establish contact with a command centre, send and gather information, update itself and perform man-in-the middle attacks.

In 2012, customers were requested by their banks to switch off the banks' log-on system (BankID) which could not be used because of a weakness in Java.

Finanstilsynet regards attacks on internet-based systems as a growing risk.

5.3 Business continuity and disaster recovery solutions

A growing number of services are regarded as time-critical. New services that require immediate processing are appearing, such as fast payment and granting of on-the-spot loans. When it comes to business continuity and disaster recovery, Finanstilsynet finds that

- the systems often do not function according to expectations
- testing the systems in their entirety presents a challenge
- the systems are not updated in pace with the upgrading of the primary system
- training is neglected
- providers are now working together better when incidents occur

The financial industry has collaborated on the development of a number of shared systems that are operated at one location. This entails a concentration of risk that may be of significance when it comes to business continuity and disaster recovery.

Finanstilsynet regards business continuity and disaster recovery contingency as a risk area.

5.4 Risk associated with old and complex systems

There are challenges associated with

- the amount of maintenance required by old systems
- the expertise on and capacity of old systems
- integration between old systems and new services
- the steadily increasing complexity of the integration stage, which gives rise to faults and downtime
- security loopholes as a result of complexity

Finanstilsynet regards the risk in this area as being on the increase.

5.5 Access to payment services

The payment services incident during Easter 2011 resulted in a comprehensive risk analysis of the financial ICT infrastructure and action to reduce the risk of incidents. Nevertheless, serious incidents have occurred in the area that has been studied. There was no decline in the number of incidents in 2012 compared with 2011.

The risk of incidents that will affect the availability of services is deemed to be at the same level as in 2011, and must continue to be monitored.

6 Further monitoring by Finanstilsynet

6.1 Supervision of IT risk and other contact with institutions

Finanstilsynet's monitoring of institutions' IT risk primarily takes the form of supervisory inspections. The purpose and scope of the inspections varies, but they are based on a risk assessment of the institution in question. The primary legal basis for supervision is the Norwegian ICT Regulation and various form-based self-evaluation modules. The most common self-evaluation forms are available on Finanstilsynet's website. On the basis of Finanstilsynet's risk assessments, examination of specific topics will be integrated into the general supervisory activity.

Finanstilsynet is otherwise in ongoing contact with the institutions in connection with the general IT risk situation, projects and incidents.

6.2 Reporting of incidents

Financial institutions are required to report significant incidents to Finanstilsynet; see Section 9 of the ICT Regulation. Such reported incidents provide insight into financial institutions' risk which Finanstilsynet may also need to follow-up. Not least, the incident database provides a valuable source for analysis of trends and relationships[31].

6.3 Work with payment systems

The legal basis for Finanstilsynet's responsibility for payment systems is the Financial Supervision Act and the regulations on risk management and internal control and on the use of ICT. Responsibilities relating to payment system services are also regulated by chapter 3 of the Payment Systems Act. There is also extensive self-regulation of this area through bank collaboration and responsibilities assigned to Finance Norway for shared services. The rules are included in the "Blue Book" on governance of banks' self-regulation. Norges Bank also has important responsibilities in connection with payment systems with legal basis in the Norges Bank Act and the Payment Systems Act. The collaboration between Norges Bank and Finanstilsynet is described in a separate memo[32], to ensure the best possible interplay in this important area. Norges Bank and Finanstilsynet also cooperate on material that forms the basis for Norges Bank's Annual Report on Payment Systems and Finanstilsynet's RAV analysis. Together the reports provide an overall picture of risk associated with payment systems and the financial sector's use of ICT.

6.4 Requirement to give notification of the establishment and operation of systems for payment services

Institutions shall notify Finanstilsynet of the establishment and operation of a system for payment services without undue delay; see section 3-2 of the Norwegian Payments Systems Act. The duty of notification is described in more detail in circular 17/2004 (Norwegian text)

[31] http://www.finanstilsynet.no/no/Tverrgaende-temasider/IT-tilsyn/

[32] Cooperative agreement between Norges Bank and Finanstilsynet on payment systems: http://www.norges-bank.no/pages/88601/betalingssystemloven_samarbeid_ansvarsdeling_NB_FT_2012.pdf

with appurtenant self-reporting form. The notifications are important for enabling Finanstilsynet to monitor the changes taking place in payment services and the operational risk related to these services.

As stated in chapter 3.2, few notifications are received, and there is reason to believe that the institutions do not comply with the requirements of the Act to a sufficient degree. To ensure compliance with the Act, Finanstilsynet is considering whether there are grounds for using the basis for regulations provided by the Payment Systems Act, and whether circular 17/2004 should be replaced by regulations.

6.5 Contingency preparedness work – Contingency Committee for Financial Infrastructure

Work is in progress through cooperation with the financial industry, Norges Bank and other authorities to ensure the necessary prioritising of electricity and telecommunications for institutions that are important for maintaining operations in key institutions in an emergency situation. Work is also in progress to ensure necessary means of payment for the population in a long-term emergency situation. This is taking place in connection with a review of important financial institutions' established contingency organisation and contingency systems and verification that the systems function by means of the documented results of disaster recovery testing.

6.5.1 The Contingency Committee for Financial infrastructure (BFI)

Contingency preparedness exercises are planned and carried out annually across financial institutions and providers under the auspices of the BFI.

The BFI is an important meeting place for different operators in Norway who have responsibilities within the Norwegian payment system. The committee has many responsibilities, but has a particular focus on contingency work, and is therefore concerned with following up incident trends. Conducting exercises in order to be optimally prepared in the event of a serious incident receives priority. Finanstilsynet will continue the work of developing the BFI and remain responsible for the chairmanship and secretariat of the committee.

FINANSTILSYNET
Postboks 1187 Sentrum
0107 Oslo
POST@FINANSTILSYNET.NO
WWW.FINANSTILSYNET.NO