Chapter 1
The Financial Critical Infrastructure and the Value of Information Sharing

Enrico Angori, Roberto Baldoni, Eliezer Dekel, Atle Dingsor, and Matteo Lucchetti

Abstract The financial system is quintessential to the functioning of a modern nation's economy. Therefore this system can be definitely considered as a critical infrastructure of our society and, due to the continuously increasing penetration of the Internet world inside this infrastructure, it has to be protected from cyber attacks. This chapter introduces the main actors forming the financial system and their relationships and analyzes the system's vulnerabilities to cyber attacks. Along this direction, the chapter investigates the financial ICT infrastructure of Norway as a case study and shows the current protection strategies adopted by financial players. The importance of information sharing at the level of a sector-specific market, such as the financial one, has been pointed out in eight added values, and examples of how poor information sharing results in sector-specific vulnerabilities are discussed. Finally some examples of information sharing methodologies are analyzed.

E. Angori
SelexElsag, Via Laurentina, Roma, Italy
e-mail: enrico.angori@elsagdatamat.com

R. Baldoni (✉)
Dipartimento di Ingegneria Informatica, Automatica e Gestionale Antonio Ruberti, Università degli Studi di Roma "La Sapienza", Via Ariosto 25, Roma, Italy
e-mail: baldoni@dis.uniroma1.it

E. Dekel
IBM, Research Division, Haifa University Campus, Mount Carmel, Haifa 31905, Israel
e-mail: eliezer.dekel@ibm.com

A. Dingsor
Kredit Tilsynet, Oslo, Norway
e-mail: Atle.Dingsor@kredittilsynet.no

M. Lucchetti
Poste Italiane, Roma, Italy
e-mail: lucch102@posteitaliane.it

R. Baldoni, G. Chockler (eds.), *Collaborative Financial Infrastructure Protection*,
DOI 10.1007/978-3-642-20420-3_1,

1.1 Introduction

The financial system comprises many entities that interact with each other to provide financial services that are the lifeline of the world economy. It is a complex landscape of actors, including stakeholders, regulatory agencies, financial service providers, and the communication networks linking them. The economic role of financial intermediates and regulators in financial markets is that of increasing welfare in the economy through efficient capital allocation and risk sharing. For example, commercial banks are basically intermediates between individuals (who deposit their funds in the bank and don't need the capital at the moment) and firms (for which the banks issue loans, as they need the capital for their operation). They serve as a pooling device in the financial markets. Clearing houses facilitate trading by mediating two traders entering a future contract. Central banks have a regulatory role; for example, the central bank requires commercial banks to hold a certain percentage of their assets as capital (capital requirement). In this chapter we review this financial system, its stakeholders, and their interrelations. We identify and classify the vulnerabilities of interconnected financial infrastructures. Specifically, the chapter includes the current state of the art of financial communications, describing its actors, its high-level needs, and the existing structures that support financial communications.

Communications form a key basis for the financial world and necessitate a high level of security and privacy. Today these requirements are fulfilled by private network and proprietary communication protocols, which guarantee the high level of security needed in financial transactions. Driven by the growing popularity of mobile commerce, the interconnections across financial institutions are growing worldwide. The need exists to consider the use of open networks as well as private and public clouds to drive this level of pervasive access while maintaining the needed security and responsiveness levels and reducing the total cost of ownership (TCO). Nowadays the new IT technologies can guarantee a high level of security and dependability; however, they are not widely used due to the actors' reluctance to use public communication networks.

The financial information and communication technologies (ICT), the interrelationships and interconnection between financial actors and regulators, are high on the agenda today, as banks played an important role in the current financial crisis. Regulations or the lack thereof were part of the problem. Banks used asset-backed securities to evade capital requirements, and when housing prices went sour, banks did not have enough capital to operate, and lending activity came to a halt. Government intervention was needed to make the banks operational again, lending to firms and other players. Research in financial infrastructure (FI) falls somewhere between the fields of finance/economics and information systems. Finance/economics needs to define the roles of financial players and the nature of the connectivity required among them. Information systems should then address how such relationships are best implemented by technological infrastructure.

In order to satisfy the requirements of the financial ecosystem, there are a number of market-specific technical requirements for responsiveness, data integrity, security, and privacy. The financial market indeed stipulates its own specific needs;

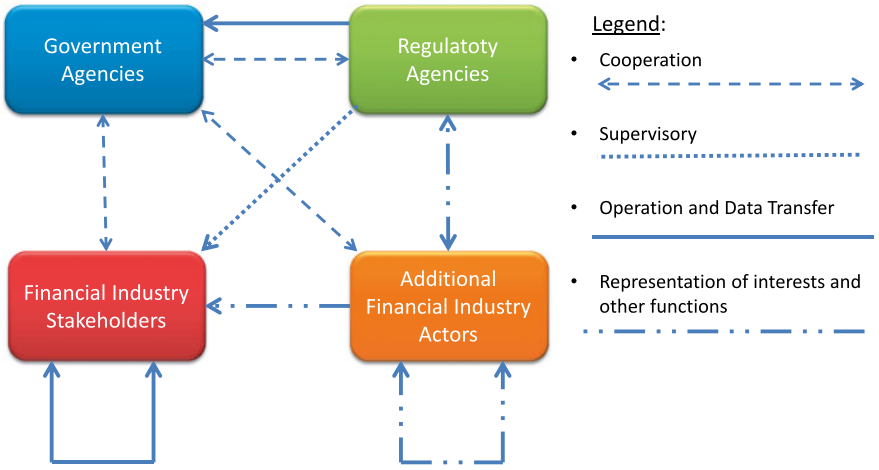

Fig. 1.1 Simplified logical connections between the players of the financial industry

therefore, software and service providers have, over time, implemented domain-specific solutions to meet them. Section 1.2 provides an overview of the financial infrastructure: the business actors, regulatory agencies, and the associated ICT and its requirements; in Sect. 1.2 we survey the main stakeholders. We then review, in Sect. 1.3, the financial system as a critical infrastructure. An overview of the ICT in use today in financial operations with examples from the Scandinavian landscape is provided in Sect. 1.4. Following this overview we discuss, in Sect. 1.5, the vulnerability of this interconnected system to cyber attacks. In Sect. 1.6, we review cyber security measures, and in Sect. 1.7, we discuss the state of the art in bank cyber security. The last part of this chapter (Sect. 1.8) discusses the value of cooperation between the financial actors for achieving cyber security.

1.2 Main Stakeholders and Players

Though each country has its own specific model for managing financial business, there exists a general model that is shared across the different European countries that are trying to converge toward a common European model. A simplified structure of the financial system is depicted in Fig. 1.1. The main groups of stakeholders are government agencies, regulatory agencies, financial industry stakeholders, and additional financial industry actors. Government agencies take part in the money transfer processes; for instance, the national central banks (NCBs) are involved in the clearing tasks, and the Bureau of Public Debt participates in the operation of the stock exchange market. Some players provide financial services, e.g., the State Treasury keeps the accounts of the state institutes (for example, the mandatory pension funds).

These functionalities require the cooperation of related stakeholders such as the NCB and the clearing house, or the State Treasury and the mandatory pension funds. In some cases there is close cooperation between participants, e.g., between the NCB and the supervisory agency, to help improve the financial culture and the awareness of the people.

Regulatory agencies have regulatory and supervisory functionalities to ensure reliable, continuous, and transparent operation of the financial markets. For instance, banks are liable for reporting created bank accounts to a supervisory authority.

The regulatory agencies are connected with different kinds of associations that are members of the additional FI actors group. The main missions of the associations are the representation, transmission, and reconciliation of interests of the institutes they stand for and communication with similar domestic and foreign institutes and agencies. For instance, supervisory agencies and banking and insurance associations can work in connection with each other; these associations usually coordinate the operation of their institutes. The other members of this group can take part in the settlement processes such as the stock exchange.

The last set is the group of FI stakeholders. This group covers the main stakeholders, except for the supervisory authorities. These stakeholders are directly involved in the operation of the settlement, clearing, and other financial services. This group is in connection with all other groups, and the participants of this group are in connection with each other as well. For example, banks connect with each other through the clearing and settlement systems, which involve data transfer between the institutes. In some cases, the bank, the insurance company, and the pension fund is operated by the same organization, thus involving close interconnection between these entities.

Figure 1.2 summarizes the main stakeholders of the financial system stemming from this general model. They can be divided into four main parts according to the scope of their activities: money markets, capital markets, funds, and insurance companies. The money markets group includes the banks and other credit institutions. The money market is where short-term obligations such as Treasury bills, commercial paper, and bankers' acceptances are bought and sold. The capital markets group consists of investment firms and fund managers. The capital market is the market for securities, where companies and governments can raise long-term funds. The funds group contains the different kinds of pension funds and the health and income replacement funds. Funds are related to handling people's savings. The last group consists of the different kinds of insurance companies and the related actors, such as brokers and consultants. Insurance brokers sell different kinds of insurances; they are in connection with several companies.

1.3 Financial Institutions as Critical Infrastructures

The importance of protecting infrastructures has greatly increased in recent years. In particular, governments and international agencies and organizations are focusing on critical infrastructures, i.e., those assets, systems, and functions vital to the

Main Groups of Stakeholders	Members	
Regulatory Agencies	Financial supervisory authorities Tax and financial control office	
Government Agencies	National Central Banks State treasuries	
FI Stakeholders	**Money Markets**	Banks
		Specialized Credit Institutions
		Co-operative Credit Institutions
		Savings Co-operatives
		Credit Co-operatives
		Financial Enterprises
	Capital Markets	Investment Firms
		Investment Fund Managers
		Other Institutions
	Funds	Private Pension Funds
		Voluntary Pension Funds
		Health and Income-Replacement Funds
	Insurance Companies	Proprietary Insurance Companies
		Mutual Insurance Companies
		Insurance brokers
		Insurance consultants

Fig. 1.2 Main stakeholders of the financial industry

smooth, safe, and peaceful operation of a society. Critical infrastructures (CIs) include those physical resources, services, and information technology facilities, networks, and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security, or economic well-being of citizens or the effective functioning of governments and/or economies [4]. These categories comprise utility infrastructure (water, gas, fuel, electricity, transportation, communication), banking and financial services, and food supply, etc. With the advent of the digital age and the Internet of Things (where everything is connected), these CIs become interrelated, interconnected, and even more accessible, both for legitimate users and for adversaries. Protecting the digital access for these CIs now has a special focus: cyber security.

The financial system described in Sect. 1.2 is a CI, as it is essential to the functioning economy of modern nations. Financial institutions, in fact, play the role of intermediaries, accepting funds from various sources and making them available as loans or investments to those who need them. Their operational effectiveness is rated in terms of how efficiently the financial system as a whole allocates resources among suppliers and users of funds to produce real goods and services [5].

During the last two decades, the infrastructure supporting the global economy has changed. In order to manage their internal processes and provide their services, CIs, and in particular financial institutions, increasingly rely on ICT systems and networks, and many of them are also connected to the public Internet. The dependency on information systems and technological infrastructures allows financial institutions to provide innovative and high-quality services, thus preserving efficiency and cost-effectiveness. However, whereas the benefits have been enormous for both public and private organizations, the CIs' increasing reliance on networked systems also poses significant risks to the critical operations and infrastructures they support. The result is a new form of CIs, generally referred to as critical information infrastructures (CIIs), that totally or partially rely on one or more information infrastructures for their monitoring, control, and management and are therefore vulnerable to new forms of cyber threats and attacks, in addition to traditional physical threats. Such technological information infrastructures must be dependable; i.e., they must guarantee availability, reliability, correctness, safety, and security, under normal working conditions and in case of an emergency, that is, when critical events occur. It is therefore crucial to protect those infrastructures and adopt strategies to guarantee that the different infrastructures are able to correctly and continuously supply their services in spite of any event [6].

Some industries and types of businesses are more susceptible to cyber-related crimes and attacks, and the risk level is particularly high for the banking industry and financial institutions. Moreover, this sector is also extremely vulnerable to public perception: an impression of weakness could easily result in a damaging cascading effect. Business continuity is therefore necessary to maintain public confidence.

Attacks targeted to financial institutions [7] are typically performed in order to:

- gain unauthorized access to sensitive or confidential information
- disrupt normal business
- create costly distractions
- steal funds
- reduce confidence

Potential damage and possible consequences that may occur when systems supporting critical financial operations are threatened include:

- services and benefits interruption
- sensitive data disclosure
- data integrity corruption
- money and information theft
- commercial structures and financial systems bankruptcy
- international business transactions failure

- markets destabilization
- unauthorized access and/or modification of personal information
- loss of confidence and reputation

It is important to adopt protection strategies and measures in order to reduce vulnerability to cyber threats, prevent cyber attacks against CIs, and minimize damage and recovery time from attacks that do occur. Taking preventive measures and improving early detection and reaction capabilities allows financial institutions to limit the effects and impact of disruptions and attacks on governments and society, and to ensure business continuity, guaranteeing that affected systems are always able to provide a minimum service level or that they can be restored within the shortest possible time.

1.4 Standard Solutions for Securing the Financial Infrastructure

Financial IT infrastructures are used to process, store, and exchange critical and sensitive information; hence they are characterized by strict security requirements. Systems, networks, data, and exchanged information should be protected against any type of malicious activity (such as interception, insertion of fake information, update, delete). The relevance of security requirements in the financial context is highlighted by the Basel II accord [8]. Damages caused by security breaches within the financial IT infrastructure fall within the operational risk category, as defined in the Basel II first pillar [9] and Annex 9 [10]. In particular, system security issues (such as hacking activities and data theft) are considered as examples of the external fraud event type, defined (among others) within the operational risks. System and network issues also represent the main focus of the standards with which financial institutions and their customers can voluntarily comply in order to obtain widely recognized international certifications, such as the Payment Card Industry Data Security Standard (PCI DSS) [11].

The financial IT infrastructure is a key critical infrastructure (CI) for financial operators and consequently must be dependable or trustworthy. The attributes of dependability/trustworthiness [12] refer to the degree of (quantifiable) user certainty that the system will operate as expected and that the system will not fail in normal use. Basically, the IT financial infrastructure must satisfy the following dependability and security requirements and properties:

- Availability: the capacity to access systems, networks, and critical data for the infrastructure survival anytime, even if the infrastructure is operating under extreme conditions.
- Reliability: the capacity to ensure that a system or network will perform its intended functions without failures when operated under specific conditions for a specified time interval.
- Authentication: the capacity to identify a user that is appropriate to the specific information and service type.

- Access control: the capacity to ensure that only authorized users can access system and network resources.
- Data and message confidentiality: the capacity to ensure that only authorized users can access protected data and messages.
- Data and message integrity: the capacity to ensure that data managed by systems and messages transmitted over the network are not altered by unauthorized users or non-guaranteed software or hardware.
- Reliable message delivery: the capacity to avoid message loss and replication and guarantee ordered delivery, along with the ability to provide verifiable proof of delivery to both the endpoints of a communication.
- Non-repudiation: the capacity to provide verifiable proof of message delivery to both the endpoints of a communication, in order to ensure that the sender of a message cannot deny having sent the message and that the recipient cannot deny having received the message.

In addition to dependability and security requirements, the financial infrastructure has to meet performance and quality of service (QoS) requirements, characterized by specific low-level technical metrics for interconnection networks (such as packet drop, network latency round trip time, jitter, out-of-order delivery, and transmission errors) as well as higher level business-level metrics (such as number of transmitted transactions, percentage of rejected transactions, and number of incorrect transactions).

The most challenging aspect in financial CII is the new model that is becoming established for financial transactions. Up to twenty years ago a financial transaction was originated by a financial stakeholder (such as a bank) and was received through a complex communication network and few intermediate nodes by another financial stakeholder (such as another bank elsewhere). Communication networks at that time were quite controlled and secure. Nowadays the new model foresees online and real-time transactions that are generated by a non-financial stakeholder (usually a business customer), flow through financial stakeholders and intermediate nodes, and sometimes arrive to another non-financial stakeholder (for example, an enterprise or an SME). In this new model the communication network includes many different network types and often includes Internet as well. In such a case the communication network cannot be considered as intrinsically controlled and secure.

Communications among financial players are carried out through quite different technological solutions providing different performance, reliability, and security levels: communications among financial institutions usually leverage dedicated leased lines; central bank offices are connected to local agencies through other dedicated lines or through secure virtual private networks (VPNs) over Internet links.

Financial organizations are nowadays interconnected through extensive proprietary networks to provide their financial customers with advanced services and to exchange financial messages securely for business purposes (e.g., cash management, fund transfers, credit advices, and alerts). These networks are for financial transactions only, and complex requirements related to security and privacy lead to proprietary and closed networks. Usually, financial networks are hierarchically interconnected according to a tree structure. In this interconnection model, each network can

be considered as a tree node at a well-defined level. Therefore, two networks standing at the same level can communicate by sending their messages to the network at the upper level, which guarantees a secure and reliable exchange of information.

Leased lines interconnecting financial institutions are specifically designed for high availability. Fault tolerance is provided by means of multiple redundancy. High dependability is also achieved through isolation of these dedicated communication lines with respect to the Internet traffic. This choice protects financial communications from availability issues. Dedicated communication lines used for information exchange among financial players can provide a tightly monitored and controlled environment, in which it is possible to enforce performance-oriented policies. In this context, the possibility of performance guarantees is a direct consequence of the isolation of the dedicated communication lines with respect to the shared Internet. In isolated networks, it is rather simple to design and provide a communication infrastructure where the performance cannot be jeopardized by uncontrollable Internet phenomena and/or attack that could result in the degradation of the communication channel performance. Moreover, the complete isolation of financial networks from other networks ensures a high level of security against intrusions or malfunctions from outside. However, it is often difficult to separate financial networks from external ones because they have the need or the convenience to interconnect to other networks to exchange essential data for financial purposes. Hence it is important to ensure maximum network interconnection security under these conditions, using suitable protection policies and technical solutions that guarantee full access and data exchange security. Financial CIIs include connections among financial institutions and their customers. While high security guarantees can be achieved through dedicated channels, communications between a financial player and their customers are carried out through the Internet. Nevertheless, it is possible to guarantee authentication, non-repudiation, privacy, and integrity by leveraging state-of-the-art encryption and key distribution algorithms. Virtual private networks (VPNs) can be established to enable secure communication between a known and authenticated user and (virtually) any host belonging to the internal network of a financial organization. This solution can be effectively used to enable secure (but not dependable) communication channels for customers or employees of a financial institution that is connected through the Internet. Transaction security is implemented at the platform and application levels, and performances usually cannot be guaranteed. Processes for establishing and securing the communication link and for managing transactions are defined by the financial institutions and then carefully implemented by the customers (such as the use of one-time passwords (OTPs) to confirm transaction).

Communications that use the Internet as a backbone cannot be characterized by performance guarantees. It is possible to stipulate service level agreements (SLAs) when there is one provider among the financial institutions or when the traffic is confined in one autonomous system. In the more general case, however, it is impossible (or very difficult) to guarantee SLA contracts when multiple autonomous systems are involved between the communication endpoints. In fact, Internet traffic can be arbitrarily delayed or dropped by intermediate autonomous systems that are based on a best effort routing service.

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is the most important worldwide financial communication infrastructure that enables the exchange of messages between banks and other financial institutions. It was founded in 1973 as a cooperative society owned by member banks. SWIFT does not generate transactions, but it is responsible for providing a fast, secure, available, and accurate means of transferring a variety of financial instructions on behalf of its international members. It is a private network which provides the platform, products, and services to connect and exchange financial information among financial organizations all over the world. Therefore, SWIFT can be considered as one of the nodes on the top of the tree model representing the interconnection structure of the European financial networks. National financial networks are lower level nodes that can be connected to SWIFT by specific backbone access points that act as communication gateways, and they can provide different services. An example of secure communication infrastructure among financial players is represented by SWIFTNet, which is a secure IP-based network to which financial players can gain direct access.

SWIFT security mechanisms helped to create a large step forward in the safe and reliable transfer of financial messages. SWIFT has numerous security advantages; thus financial institutions opted for the SWIFT network, rather than the traditional (and much less secure) Telex instruction, as a preferred method of transfer. Currently SWIFT has changed to its IP network infrastructure, known as SWIFTNet, totally replacing the previous X.25 infrastructure.

Basically, SWIFT provides a centralized store-and-forward mechanism including transaction management. Bank A, which needs to send a message to bank B with an authorization of institution C, formats the message according to a well-defined standard and securely sends it to SWIFTNet. SWIFT guarantees secure and reliable delivery of the message to bank B after the appropriate action of institution C.

1.5 Financial ICT Infrastructure in Norway: Tradition of Cooperation and Associated Risks

Norway FIs and customers are heavily dependent on the Internet. As of January 2011, there were close to 5 million signed agreements for the use of Internet banking. Norway has a population of approximately 5 million. The number of invoices paid through Internet banking increased by 5.6 percent last year (2010). More than 90% of all invoices being paid in Norway are paid using Internet banking.

There were 70 million ATM withdrawals in Norway in 2010, down by 25 percent over the last five years. An increasing number of Norwegians use mobile banking services, such as mobile banking, bank applications (apps) for iPhone and other smartphones, as well as Short Message Service (SMS).

Norwegian banks traditionally have pooled resources and jointly developed systems in key areas. There is a bank-wide debit card system. Each bank issues debit cards under its own brand. Merchants are customers of a bank of their choosing. A card issued by one bank may be used interchangeably at any point of sale (POS)

terminal. The debit card may also be used at any ATM, regardless of which bank owns the ATM. There is a common scheme for checking PINs and a common scheme for checking an account balance and making reservations against the balance. The banks have common procedures for dealing with offline situations.

There is a bank-wide e-invoice system in Norway. The payment information is held in one bank-wide database, which also contains information about which Internet bank(s) the customer uses. Any e-invoice is sent to the Internet bank(s) of the customer. The customer may pay the e-invoice through any of her Internet banks. Any other Internet banks that the customer may use are automatically updated to reflect that payment has taken place; i.e., the e-invoice is no longer shown as pending.

Likewise, the banks have worked together to develop a system for standing orders. The beneficiary enters into an agreement with her bank to the effect that the beneficiary will offer the payer the option of paying by a standing order. Information that the beneficiary offers regarding the standing order payment is made available to all banks. Hence, on entering payment details of the beneficiary the first time, the payer is informed by her Internet bank that she may enter into a standing order agreement. The payer sets a maximum amount per invoice applicable under the agreement, and may cancel it at her discretion. The infrastructure for this transaction is developed jointly by the banks.

The banks have also jointly developed an authentication system for the Internet, called BankID. Each bank is a separate certificate-issuing authority. User private keys are stored centrally on hardware and premises shared among the banks. The user enters a user ID, an OTP, and a fixed password, which is consumed by a signed applet and communicated to the central security server for access to the private key. The user may authenticate to a number of web sites using her BankID. Given the increasing number of web sites asking for BankID authentication, there is a risk that the user may be less critical with respect to whom to submit authentication credentials, which would increase the risk of phishing and other attacks against the ID. Securities trading is increasingly done over the Internet, through Internet banks or stand-alone brokers. These examples illustrate that there is a strong tradition for cooperation and information sharing and for joint systems development among Norwegian banks.

A comparison among members of the IT Security Group (ITSG) reveals that Norwegian banks are heavily outsourced. Within Norway, a few “hubs” supply the bulk of banks with IT services. One bank has its corporate IT operation in Sweden, supplied by IBM. Two other bank groups are outsourced to Denmark; IBM is the main IT supplier.

As a consequence of being heavily outsourced, IT skill in the FIs is probably deteriorating. It is difficult to uphold procurement skill in FIs, when the FI is not involved day to day in the IT operation. It is particularly disturbing that IT risk probably also would be less understood and acknowledged under these circumstances. As the specialist, the supplier’s view carries a lot of weight and the supplier’s arguments often override arguments internally within the FI itself. However, the supplier might have a different perspective than the FI. Based on years of observation, we would like to point out the following. Firstly, IT suppliers tend to have a shorter

term perspective than the FIs when it comes to the company's bottom line. The suppliers may not have the right incentives to invest long term in security up front. Secondly, IT suppliers may not fully understand and acknowledge that IT security is of prime concern and should permeate all IT development and operation. Thirdly, the supplier may not be fully aware of the concentration risk to national critical infrastructure that arises from serving several FIs on the same system. Recently, supervisors noticed that a microcode error reported on one CPU with a key supplier in Norway seemed to coincide with irregular service reported by the majority of banks in Norway. The seriousness and symptoms varied among the banks. The supplier indicated that not all banks were served by the CPU in question; rather banks were spread across CPUs. On further investigation it turned out that the banks were indeed in some way or other dependent on the malfunctioning CPU. Hence a serious concentration risk was discovered.

In 2010 a key supplier had aggressive plans for outsourcing IT operations to Ukraine and to India. Apparently this made for a good business case, and the banks were about to accept the arguments from the supplier more or less at face value. The supervisors questioned some aspects related to control, governance, integrity, and availability of information processed and stored off-shore. Ukraine scores high on Transparency International's corruption index. The supervisors felt that the prospect of the outsourced financial institution having to resort to nontraditional payment methods in order to renew the lease on the data premises or to get more bandwidth from the local telecom supplier was somehow not to be desired. The supervisory authority issued a statement to this effect, and the statement contained other warnings as well. After further study, the FIs seem to have withdrawn their plans for off-shoring.

The arguments above indicate that there is an inherent risk that FIs are gradually leaving more decisions in the hands of the IT suppliers. Also, the market for supplier services is very thin; in key areas there will be only one or a few suppliers. Because there are few practices to compare, it is hard for the FIs to establish what is "best practice", which poses the danger of the FIs becoming less critical than they should be.

Being outsourced for a number of years, the FIs are heavily embedded in the supplier software and hardware. Running time-critical systems around the clock, the idea of changing suppliers seems like a daunting one. It is to be expected that FIs feel uncomfortably locked in under these circumstances, and that suppliers drive the FIs, rather than the other way around.

1.6 Vulnerabilities to Cyber Attacks

FI services are becoming more automated. Several suppliers, systems, protocols, and carriers (mobile, IP, voice) are involved. The experience of the supervisory authority tells us that the interfaces between suppliers are particularly risky areas. The interface may involve protocol conversion, format conversion, decryption and re-encryption, scheduling, etc. An example would be mobile banking. Transactions are

carried over GSM and IP networks on their way from the handset to the bank. This calls for decryption of the GSM payload once it hits the mobile server, and then re-encryption to facilitate further IP transmission to the bank. At this conversion point, the traffic is exposed. This calls for some sort of end-to-end encryption on a higher (application) level, which in turn may be hard to realize given the plethora of different handsets. Key management may be hard to administer.

The risk is amplified as the transactions chains become longer, bringing together different technologies. Recently banks have introduced online loan application and processing. At the other end of the transaction chain, encrypted personal online storage facilities are being offered, like an electronic security deposit box. Let's say you apply electronically for a loan, maybe using your handset. The loan is being processed electronically, involving communication with various non-bank authorities, e.g., notaries, real-estate registrars, credit information agencies, tax authorities, and marital registers. The loan is granted and discounted. All pertinent documents and information are stored in the electronic storage of the customer and the bank. At various steps along the way digital authentication and signing takes place, probably involving different authentication mechanisms and different suppliers. Given the complexity of the chain of events, there is a substantial risk of something going wrong. Upholding confidentiality requirements is one of the challenges. The last year has seen several incidents of unwanted exposure of confidential information.

Eventually, the customers themselves are part of the cyber security problem. Viruses, Trojans, and any other type of malware may infect an unprotected endpoint, stealing information required to complete a financial transaction. The whole process that was agreed on and established to secure financial transactions (such as connection to an https site, use of credentials to identify and authenticate the customer, personal information for further user identification) is implemented by the customer and may be compromised by wrong customer behavior. Phishing and other similar techniques are examples of these types of threats that impact cyber security.

Vulnerability analyses over the whole service chain are complex tasks. Where are the weak points?

1.7 Security Systems and Technologies

A secure FI includes several software solutions providing tools to prevent, recognize, resist, tolerate, and recover from events that intentionally or accidentally threaten the dependability of the infrastructure. In order to secure IT systems and networks and protect FIs from cyber attacks and other threats, a wide range of security technologies is used. These include access control technologies, system integrity technologies, audit and monitoring tools, and configuration management technologies. Security solutions have three main objectives, which are all critical for properly protecting financial infrastructures:

1. *Prevention*: Preventive activities aim at stopping a fault from occurring or an attack from succeeding. Preventing security breaches is possible only for well-known vulnerabilities.
2. *Detection*: Despite preventive activities, new attacks can occur because of newly found vulnerabilities or attack techniques. Detection activities aim at identifying that a security breach has occurred. In order to properly react, detection should be achieved in real time.
3. *Reaction*: Once a security breach has been detected, reaction activities aim at stopping the attack, mitigating the effects, and reducing the damage it has caused. Reaction activities may include the collection of detailed information in order to prevent and detect attacks in the future.

The following paragraphs provide an overview of the main security technologies and solutions. A detailed analysis on how the specific technologies work can be found in [13].

Identity and access management: tools that provide a secure, automated, and policy-based user management platform supporting user access control, authentication, and authorization. In order to protect internal systems, networks, and data, access control technologies ensure that only authorized users can access protected information and resources. In particular, authentication technologies associate a user with a specific identity. Users can be authenticated by different methods, including shared secret systems, digital certificates, token-based systems, and biometrics. Authorization technologies manage user rights and privileges in order to grant or deny access to a protected resource (a network, a system, an individual computer, a program, a file, etc.). Operating systems and sensitive or mission-critical applications incorporate appropriate access controls that restrict which application functions are available to users.

Transaction control: tools that implement a structured process to control transactions, for example, by using off-band communication. These tools may be used to reinforce transaction input by using two separate communication channels (for example, Internet connection and mobile device). In this way a transaction is started using one channel (for example, a web-based windows operating over the Internet) and is then confirmed using the other channel (an SMS message to a customer mobile number). This process is based on the idea that compromising two separate channels is much more complex than compromising one.

Network access control: tools that protect the logical or physical boundary of a network, in order to prevent access to the network by external unauthorized users. Network access control technologies include firewalls and network-based intrusion prevention systems (NIPSs). Basically, firewalls block or allow network traffic based on static or dynamic rules configured by the network administrator. A NIPS allows or disallows access based on an analysis of packet headers and packet payloads. The NIPS can detect security events and, after detection of malicious activities, may take specific actions, such as blocking traffic flows. A NIPS not only can detect an intrusive activity, it also can attempt to stop it.

Application monitoring: tools that monitor performance and availability of the applications and services running on the servers. In particular, they perform monitoring of hardware (CPU utilization, memory, disk space, etc.) and software components and monitoring of operating systems status. Collected data may be used for historical reporting, performance analysis, trend prediction, and other data mining activities. Application monitoring tools typically provide web-based interfaces and alerting mechanisms for notifying administrators about potential issues.

Network management and monitoring: tools that are able to automatically discover devices and hosts on a network, build a routing map to reflect network logical organization, and display network topology. They provide support for fault management (i.e., identification of network failures), configuration management (i.e., monitoring of network configuration information), and performance management. Network management and monitoring tools typically provide a centralized management console for event visualization and network diagnostics.

Data and storage management: tools that provide a platform for managing complex storage in distributed heterogeneous environments. They are able to protect and manage a broad range of data, from workstations to corporate server environments. Provided functionalities include centralized administration of data and storage management, fully automated data protection, efficient management of information, and automated high-speed server recovery. In addition, data and storage management tools protect an organization's data against hardware failures and other errors by storing backup copies of data in an offline repository.

Activity monitoring: tools that perform host and network data gathering and analysis in order to identify security-related events and anomalous behavior that may indicate an intrusion or an ongoing attack. Activity monitoring tools include network-based intrusion detection systems (NIDSs), deep packet inspection (DPI), honeypots, and host-based intrusion detection systems (HIDSs). NIDSs and HIDSs are able to identify potential attacks and intrusions using predefined signature or anomaly detection techniques, and may take predefined response actions. A honeypot is a network device that an institution uses to attract attackers to a harmless and monitored area of the network. DPI is a form of computer network packet filtering that examines packets as they pass an inspection point, searching for protocol noncompliance, viruses, spam, intrusions, or predefined criteria. Once the DPI detects a suspicious behavior, it can generate an event to an analytics tool or it can decide not to allow the packet to pass.

Configuration management and assurance: technologies that support security administrators to view and change the security settings on hosts and networks, verify the correctness of the security settings, and maintain continuity of operations and services. Configuration management and assurance technologies include policy enforcement tools, continuity of operations tools, and patch management. Policy enforcement technologies allow system administrators to perform centralized monitoring of compliance with the institution's security policies. These tools examine desktop and server configurations that define authorized access to specified devices,

compare these settings against a baseline policy, and provide multilevel reports on computer configurations. Continuity of operations tools, which adopt clustering, load balancing, and replication techniques, provide a complete backup infrastructure that increases fault tolerance to keep the institution's services online and available at multiple locations in case of an emergency or planned maintenance. Patch management tools automate the otherwise manual process of acquiring, testing, and applying patches to multiple computer systems.

System integrity: tools used to ensure that a system and its data are not illicitly modified or corrupted by malicious code. System integrity tools include antivirus software and integrity checkers. Antivirus software, using specific scanners, provides protection against viruses and malicious code, such as worms and Trojan horses, by detecting and removing the malicious code and by preventing unwanted effects and repairing damage that may have resulted. File integrity checkers are software programs that monitor alterations to files that are considered critical to either the organization or the operation of a computer, by comparing the state of a file system against a trusted state, or a baseline, built using one-way hash functions.

Virtual private networks (VPNs): use cryptography to establish a secure communication link across unprotected networks (e.g., the Internet), allowing connection between two or more remote physical locations. Data privacy is maintained through security procedures and protocols, such as tunneling, IPSec, and Secure Sockets Layer (SSL), that encrypt communications between two endpoints.

Online and offline analytics: tools for identifying and recognizing anomalous behavior patterns. In order to detect attacks, malware, potentially dangerous misconfigurations, and internal misuse, a security team must analyze a huge amount of event data coming from the different components of the security infrastructure (e.g., intrusion detection systems, firewalls, VPNs, and antivirus applications). Since analyzing logs and or events produced by a single device is insufficient to gain a full understanding of all system activity, sophisticated attacks and intrusion techniques may be detectable only by correlating events and logs produced by several security systems and devices. Unfortunately, the huge volume of data and the number of machines in a typical network can make manual analysis of security data impossible. Therefore, it is important to automate the process of aggregating events from disparate devices and systems into one logical central location, where the data can be correlated in order to simplify incident response and reporting. In order to automate the process of aggregating and correlating events, financial institutions typically deploy security information and event management (SIEM) systems within their domains.

1.8 Financial Systems Protection Strategies

1.8.1 Online Protection

This section covers protection strategies that aim at preventing attacks from having any effect. The strategies typically are twofold. The first strategy is to accept that a

particular service is indeed vulnerable, and counter this vulnerability by making the potential rewards from an attack as small as possible. Another strategy is to reduce the vulnerability to near zero. Both strategies would make it unattractive to attack the service, and one could expect that attacks would not occur. In the next section, on the other hand, we explore protection strategies that are targeted to specific ongoing attacks, i.e., protection strategies that aim to isolate, contain, mitigate, and stop an attack.

The use of standing orders is increasing. A standing order is an agreement between a bank and its customer that the bank shall automatically effect payments, i.e., debit the customer's account and send a corresponding credit instruction to the creditor bank. There is one agreement for each debtor/creditor pair. The agreement often sets a limit as to the value of each payment. The agreement is running; i.e., one and the same agreement applies to repeat payments until the agreement is canceled by the customer. The creditor must also enter into an agreement with her bank. A perpetrator would have to be accepted as a legitimate creditor for standing order payments as a first step in defrauding customers. The payments are effected automatically based on information stored centrally with the banks. The customer does not have to be logged on for the payment to take place. Hence there is limited scope for a Trojan, Man in the Middle (MitM), or Man in the Browser (MitB) when it comes to modifying transaction information. Increasing use of standing orders would limit the playing ground for fraudsters.

The use of e-invoicing is slowly increasing in Europe. With e-invoicing, all payment instruction information is made available to the customer through the Internet bank. In other words, the customer does not enter payment information such as amounts or credit account number. The customer either accepts the e-invoice or declines it. The creditor and debtor must enter into agreements with their respective banks in order to set up e-invoicing.

With both standing orders and e-invoicing the payer does not enter payment information, and there is very little scope for a perpetrator to modify payment information. Some countries, such as Singapore, have taken this even further by mandating each customer to predefine a list of creditor accounts to which payments may be effected. Additional security applies if the list needs to be updated, typically using out-of-band mechanisms like SMS. Needless to say, the prospect of transferring funds to an account on a list determined by the account holder would seem unappealing to most perpetrators. There is little scope for an MitM, MitB or a Trojan to do much harm.

Several banks now use a one-time password (OTP) in connection with customer log-in to the Internet bank. The primary idea is that once the customer is logged in, no impostor who has phished or otherwise obtained access to the code may log in using the same code. However, by using somewhat advanced phishing schemes, impostors have been able to get access to the code before it reaches the bank. One instance of a scheme took this close to full automation, in that attackers presented banking customers with an automated front-end to the banking application, through which the log-in occurred, giving the attackers full access to the customer account. In order to combat this kind of attack, some banks have introduced transaction authentication; i.e., the customer must enter a separate OTP upon submitting each

transaction, after and in addition to the OTP submitted in connection with log-in to the Internet bank. However, many OTP tokens (the devices that produce OTPs) are time synchronized with the machine that hosts the Internet bank. Because clocks tend to differ slightly, and to allow for time to transmit and process the code, there is a time window within which an OTP is valid. This time window allows attackers to phish two codes that subsequently prove to be valid; one for log-in and one for authenticating a (fraudulent) transaction. One could also foresee a more advanced attack, where the fraudsters have made a copy of the entire payment sequence which is played up to the customer, while the fraudster simultaneously has an ongoing session with the Internet bank, using the codes that the customer submits to the false pages. However, OTPs are good for one thing; they are a deterrent to a pent-up, massive attack. It would not be possible for an attacker to harvest OTPs and store them for a later run on the bank accounts; the OTPs would not be valid.

Several banks now offer free antivirus software for customers to download and run on their computers. The offering has a prominent position on the home page of the banks, and customers are strongly encouraged to download it. Antivirus vendors are engaged in an arms race against malware producers, and they are up against a well-organized and resourceful adversary. Lately we have seen the merger of two malware producers (SpyEye and Zeus). Advanced malware, e.g., polymorphous variants, change their signature dynamically and escape antivirus software. Hence the effectiveness and efficiency of antivirus software is being questioned. In the aftermath of an attack against Norwegian online banking customers, security analysts reported that more than half of the investigated systems infected were running fully updated application and OS versions. To a certain extent it is possible from the server side of Internet banking to harness the browser session, i.e., to harden the browser session against attacks. Before any log-in or other transactions take place, all unnecessary browser functions are turned off. Exits from the browser to external programs are disabled, handles are disabled, and so forth. The idea is that banking customers are protected against Trojan attacks even when using an infected PC and even when the actual Trojan is configured to behave in a new and unexpected way, like polymorphous viruses. Several security vendors offer solutions in this area.

In order to become aware of and stop unauthorized transactions, banks perform back-end transaction analyses, both “on the fly” and retrospectively. In a recent wave of attacks against banks in Norway, back-end analyses are known to have prevented losses. Transactions were compared against black lists of accounts. The footprint of the Trojan was identified, and transactions that matched the footprint were stopped. Some companies are proficient in collecting traces and indications that authentication credentials have been compromised. The companies post these traces to drop sites which contain profiles of compromised users. Several banks scan these drop sites regularly for traces of compromised customers. In November 2010 one prominent UK bank came across traces indicating that customers of a Norwegian bank might have been compromised. The UK bank alerted the Norwegian bank and, thanks to this early warning, the Norwegian bank was able to limit the detrimental consequences of the attack. Also, upon further investigation the Norwegian

bank found reason to believe that other Norwegian banks suffered compromised customers as well, and duly warned the banks. This is a vivid example of vigilance exercised by banks, and also illustrates the positive proactive attitude of cooperation among banks when it comes to security.

Several banks subscribe to a Computer Emergency Response Team (CERT). In several countries CERTs are government bodies. CERTs are manned with highly qualified technicians who analyze traffic and traffic patterns, looking for possible attacks. In a recent attack in Norway, the Norwegian national CERT played a prominent role in analyzing the Trojan and also in using its power to convince the ISPs to close down IP addresses of the command and control center of the Trojan.

The Banks try to educate customers. In a prominent place on their web sites, the Banks inform the customers on how to avoid becoming victims of attacks. This seems to have some effect. Norwegian banks recently experienced a massive e-mail phishing attack. Approximately 100,000 customers of one Norwegian bank received an e-mail containing a link to a phishing web site asking the customer to enter her log-in credentials, allegedly so that the credential could be verified. Many customers reported to the bank that they had been subject to a phishing attack, and very few had submitted their log-in credentials to the phishing site. The bank itself attributes this partly to the public being aware and alert, and partly to the fact that the wording in the e-mail did not fully comply with idiomatic Norwegian.

1.8.2 On-demand Protection Measures

In certain countries Internet banks use solutions for authenticating customers that are also used to authenticate the customers in other web sites [16]; that is, there is one authentication server serving all sites. The solution often employs OTP codes as part of the authentication. This implies that any OTP code would be valid for any one of the web sites, including the Internet bank. As the authentication solution gains ground, more and more web sites ask customers for their credentials. Previously the authentication credentials were submitted in the context of the Internet bank only. Now, people are being prompted for log-in credentials in different contexts, e.g., for various online shops, for log-in to public services, etc. Under these new circumstances, it is harder for the public to exercise vigilance and ask, "Who is behind this web site asking for my credentials?" Because they cannot exercise control, people will tend to become less critical regarding to whom they submit log-in credentials. This provides a case for phishing. An attacker could purport to be an online shop and phish log-in credentials and then use the credentials to log into the Internet bank. Or a web site which is authorized to accept credentials for authentication could use the credentials for unauthorized purposes, defrauding the customer. In order to combat this threat, the organization behind the authentication solution has come up with the idea of a context-sensitive OTP. This means that the OTP will be issued per web site; i.e., a phished OTP would be valid only in the context of one particular web site. An OTP obtained in connection with online shopping could not be used to log on to an online bank. This would remove the prime motivation for the phisher.

Many online banking authentication solutions are roaming; i.e., the customer may gain access to her Internet bank from PCs anywhere using the same authentication mechanism. This provides a case for phishing, inasmuch as the phished authentication credentials may be instantly used by the attacker from his PC. To counter this portability aspect of authentication, banks are known to build a table with Media Access Control (MAC) addresses and matching log-on IDs; they build this table by recording the MACs that the user regularly uses. If there is an attack, by looking up in this table, for any one customer the bank would check the MAC address and allow access only from this address or a limited number of other machines that the customer has been using.

1.9 Information Sharing for Infrastructure Protection

The need to protect CIs from all hazards (including both natural and man-made disasters and terrorism, as well as cyber-related threat or large-scale physical attacks) has been widely recognized in the US, especially after 9/11. The American Presidential Decision Directive 63 (PDD-63) of May 1998, updated in 2003 by the Homeland Security Presidential Directive 7, set up a national program of critical infrastructure protection (CIP) [2], and the federal government asked each CI sector to establish sector-specific information sharing organizations to share information, within each sector, about threats and vulnerabilities to that sector. In response, many sectors established Information Sharing and Analysis Centers (ISACs) to meet this need.

An ISAC [3] is defined as a trusted, sector-specific entity which performs the following functions:

- provides to its constituency a 24/7 secure operating capability that establishes specific information sharing/intelligence requirements for incidents, threats, and vulnerabilities
- collects, analyzes, and disseminates alerts and incident reports to its membership based on its sector focused subject matter analytical expertise
- helps the government understand impacts for its sector
- provides an electronic, trusted capability for its membership to exchange and share information on cyber, physical, and all other threats in order to defend the critical infrastructure
- shares and provides analytical support to government and other ISACs regarding technical sector details and mutual information sharing and assistance during actual or potential sector disruptions caused by intentional, accidental, or natural events

Today there are fourteen ISACs for CI including the Financial Services, Electric, Energy, and Surface Transportation sectors. When considered collectively, the individual private/public sector ISACs cover approximately 85% of the US CI.

There are ample real-world cases of cyber attacks against financial institutions with potentially grave consequences for the institutions as such and society at large.

The London Stock Exchange (LSE) is reporting (http://www.v3.co.uk/v3-uk/news/2031245/london-stock-exchange-cyber-attack) that the LSE and an unspecified US stock exchange were targeted by attackers intending to disrupt the markets. The LSE is investigating an attack at its headquarters last year; the US exchange has attributed an attack on its system to Russia. A May 6, 2010 flash crash (a large, short-lived decline in prices) saw the Dow Jones Industrial Average plummet 1000 points in one day. A similar event occurred at the LSE in August 2010. It has been claimed that the LSE systems are not Internet based, but such claims often are misleading. As was pointed out earlier, financial systems are interconnected. For example, a system is often being maintained remotely by means of devices that are connected to the Internet.

The Financial Services Information Sharing and Analysis Center (FS/ISAC) was established in 1999 by the Financial Services sector in response to the PDD-63 to enhance that sector's ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents, and to serve as the primary communications channel for the sector [1]. There are six levels of service, ranging from Basic Participants to Platinum Founding Members. The FS/ISAC is owned by its members. The FS/ISAC Board of Directors, elected by the membership, determines member eligibility, enforces member eligibility verification through trusted third parties, and oversees the operation of the FS/ISAC.

The mission of the FS/ISAC is to facilitate sharing of information pertaining to physical and cyber threats, vulnerabilities, incidents, and potential protective measures and practices, and to disseminate trusted and timely information intended to increase sector-wide knowledge about physical and cyber security operational risks faced by the Financial Services sector.

All incoming information is sent to analysts for reviewing and scoring. Collected data is analyzed in the ISAC's Secure Operations Center (SOC) by financial services sector experts to determine technical validity, indications of a broader problem, trends, etc. A team of analysts and security professionals within the FS/ISAC assess each submission regarding the seriousness of the vulnerability or attack to identify patterns. Once a vulnerability or incident is analyzed, it can be categorized as Normal, Urgent, or Crisis, depending on the risk to the Financial Services sector. After the analysis, alerts are delivered to participants. Participants will receive Crisis and Urgent alert notifications within 15 minutes after receipt by the SOC. Alerts typically contain not only the details of the threat but also information about how to mitigate the threat.

Alert dissemination to participants is supported by the Critical Infrastructure Notification System (CINS), which allows critical alerts to be sent to multiple recipients near simultaneously, as well as to provide user authentication and confirmed delivery. The system uses multiple mediums including landline telephone, cellular telephone, pager, e-mail, and Short Message Service (SMS) messaging. Participants receiving Crisis or Urgent alert notifications must access the FS/ISAC web site for specific information relating to these notifications using their access credentials to log on and authenticate themselves. Each member is associated with a user profile that allows for filtering of notifications in order to receive advisement only when a relevant issue arises, and ensure that only meaningful alerts are delivered.

FS/ISAC members may regularly search and retrieve information from the FS/ISAC database. Information in the database is available via secure, encrypted web-based connections only to authorized members at the appropriate service level. Information available through the web site includes new threats and vulnerabilities, geographic distribution of attack sources, real-time news feeds, and other relevant data.

In order to deliver the FS/ISAC services to the members, FS/ISAC has established a business relationship with a service provider, represented by VeriSign. The FS/ISAC and the service provider have a formal SLA for the various services. The status of the IT infrastructure that supports FS/ISAC services and hosts the web portal is continuously and actively monitored, and on at least an annual basis a formal, documented penetration test of the web portal is performed by a third party.

The value of the information sharing for facilitating early intrusion and fraud detection cannot be overstated. Modern cyber security relies on analytics (see Sect. 1.7), and the identification of suspicious patterns is expedited combining information from multiple sources. Below we elaborate on how banks and society at large may derive value from cooperating and exchanging data.

1.9.1 Value n.1: Based on a Real-World Example Illustrating Potential Benefits

In late 2010 one bank was alerted that items on a drop list indicated that attackers were targeting the bank's customers. Figure 1.3 shows a log of some of the events and steps taken by the bank in order to combat the attack. Note that not all events are listed, as will be evident from the broken number sequence in column one.

With the risk of losing out on the subtleties of this attack, the brief list of events shown in Fig. 1.3 in itself gives rise to afterthoughts:

- The list of events shows that eight days go by and still the attack is not contained—on day eight newly compromised IDs are posted to the drop site.
- Bank 2 seems to be more mature and knowledgeable when it comes to handling malware. On its own initiative, Bank 2 alerts Bank 1 and makes its expertise available to Bank 1. The cyber police bring in expertise on how the malware works and consequently on how countermeasures should be designed. This leads one to think that if Bank 2 and the cyber police had coordinated their efforts early on, the lead time for developing effective countermeasures might have been shorter.
- The cooperation between the banks and between the banks and the cyber police seems informal and based more or less on good will. One cannot help thinking that a more formal cooperation and exchange of information might further benefit the parties involved. Countermeasures might then be ready at an earlier stage, reducing detrimental consequences of attacks and protecting society as a whole against attacks.

Event #	Day #	Time	Event
1	1	14:48	Bank1 is notified about infections
3	1	16:05	Logon attempt from UK IP
4	1	16:35	Bank2 sends Bank1 link to drop site
5	2	09:00	Bank 1 analyzes the information received from Bank 2
6	2	09:10	Bank 1 comes across login information of customers of Bank 3, and duly warns Bank 3.
16	3	13:04	Bank 1 analyzes the configuration file of the infection that Bank 1 has received from Bank 2.
17	3	18:45	Customer records are collected from drop site
20	3	20:56	Analysis of the configuration file reveals how the customer may recognize if the PC is infected.
26	4	09:10	The certificates of compromised customers are revoked.
29	4	09:16	The recent transaction history of compromised customers is analyzed.
37	4	12:38	The Financial Supervisory Authority of Norway is notified of the attack.
45	4	13:04	All certificates of compromised customers are revoked.
47	4	13:10	There is a successful logon from a PC in UK.
48	4	13:43	The infected PCs of compromised customers are collected.
53	4	14:10	There are telephone calls with the cyber police.
78	7	10:55	Bank1 receives samples of the Zeus virus from the cyber police.
81	7	12:02	Discussions with the cyber police about how the Zeus virus works.
104	8	09:21	New “stolen” login credentials are posted to drop site.
…	…	…	…

Fig. 1.3 Anatomy of an attack

1.9.2 Value n.2: Knowledge Dissemination

Many times it is hard to determine what to look for (hard to find the attack signature). Cooperation may help determine the signature early on. Malware authors go to great lengths in programming the malware so that it is difficult to discover the malware, it is difficult to remove, and it is hard to unravel how it works, e.g., the IP of the command and control center. The configuration file is encrypted several times. In one recent attack with SpyEye malware, the configuration file was encrypted twice. After being decrypted, the cleartext revealed that the malware targeted nearly 90 different banks. Hence there is a case for cooperation when it comes to analyzing malware attacks in that all copies of the configuration file will disclose which banks are targeted.

1.9.3 Value n.3: Increase Likelihood of Discovery

Looking at aggregated data from several banks may increase the likelihood of discovering an attack as compared to looking at data from one bank only. Aggregated data may show that there are multiple attempts originating from one and the same IP address to break into different Internet banks. In order to discover this, you would have to have data from more than one bank.

Cards being issued by different issuers belonging to one person being used in two different parts of the world at around the same time would be an indication of card fraud. It would take data from several issuers to see this.

The list of examples may be extended; the point is that not only the volume of data itself would increase the likelihood of discovery. Some attacks you simply cannot unravel looking at one bank in isolation, whereas looking at data from several banks would make the attack stand out.

1.9.4 Value n.4: Illicit Transactions That Span Banks

Money laundering is the act of passing illicit money through the payment system in an attempt to "wash off stains" from illegal actions of the money. One way to do this is to pass the money through a long chain of transferals and obfuscate the source of the money on the way so that in the end the illegal origin is no longer visible. Hence the money is being transferred between accounts, banks, and even countries. To trace this long chain of transferals banks will have to cooperate. Pooling data from several banks and analyzing the data could well reveal transfer patterns that seem to have no other purpose than to obfuscate the origin.

1.9.5 Value n.5: Shared Platform for Systems Development (Extended Applications)

Banks may find it beneficial to pool resources and develop applications together. For a number of years banks in Norway have developed applications together in several areas. Recently the banks developed a common system for authentication to be used by web sites, Internet banks being example sites. In this system there is one national authentication server. The user experience is that one and the same user ID is used for all web sites. Banks in Norway have also developed a national debit card scheme; card issued by any bank is accepted at all ATM and POS terminals, regardless of which bank is responsible for the terminal. There have been a number of similar joint development projects; examples are:

- e-invoicing business to business [15]
- debit cards
- clearing systems
- systems for standing orders

1.9.6 Value n.6: Economies of Scale

Substantial resources are being spent daily by FIs on security. It seems to be a common position among FIs that security is not a competition issue. In many areas,

such as Internet banking, FIs face basically identical threats. Hence there is a case for cooperation in this area; potentially there are huge economies of scale to be had.

In the example of the recent attack against Norwegian banks, the banks claim unanimously that the coordination that took place was of great value to them. The first bank that was hit alerted the other banks, which raised their alert level. Once the encrypted configuration file was broken into, information about which banks were listed in the configuration file was swiftly distributed to the relevant banks. Transfers through the SWIFT system in all banks were monitored closely. Automated processing was switched off, and transactions were manually controlled before submitting them. One fraudulent transaction was sent over the SWIFT network to an account in a Portuguese bank. The Portuguese bank was alerted, and the transaction was reversed.

1.9.7 Value n.7: Aggregate Threat Picture

It takes time and resources to develop protection strategies against cyber threats. In order to be prepared, it is important that the FIs have detailed knowledge about the threat so that they may develop strategies to neutralize it. In the absence of coordination, each FI would monitor report and treat threats and attacks in its own individual way. We find that the different forms, formats, descriptions, and classifications that exist between FIs make it almost impossible to aggregate statistics to arrive at a composite threat picture for a region, country, or business type. Recognizing this challenge, in Norway there has been an effort to harmonize the reporting of credit card losses, Internet banking losses, and undesirable events occurring within the EDP operation of the banks. The work so far has proven fruitful inasmuch as there is now a better understanding of the overall loss and incident situation in Norway. But there still is a long way to go. Needless to say, if low-level traffic data from all banks were subject to massive analysis, it would be much easier to arrive at a uniform, composite threat picture that would reflect on the situation within all participating banks. This could be used to furnish supervisors on a country level or EU level with a near-time, precise threat picture.

1.9.8 Value n.8: Uniform Reporting

Post the 2008 financial crash, the reporting burden has increased. Reports today come in disparate form, format, timeliness, and accuracy. Our recommendation is to pool resources, set up a development bed, and develop jointly uniform reporting systems. Then arrive at an aggregate report on a national/EU level.

Fig. 1.4 Proper log-in page of DBS Bank

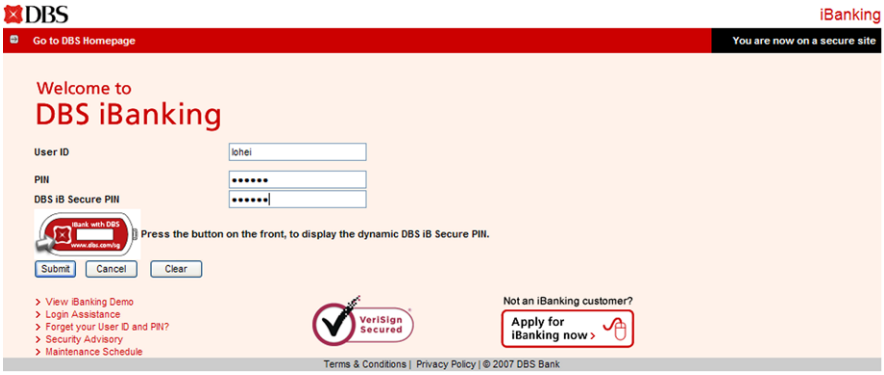

Fig. 1.5 Log-in page of DBS Bank produced by the malware

1.10 Collaboration and Information Sharing Between Banks: A Case Study

In February 2011 customers of several Norwegian banks were infected with SpyZeus, a powerful malware. SpyZeus is the result of a recent merger between SpyEye and ZeuS. SpyEye, which does much the same thing as ZeuS, came on strong in 2010 as a competitive rival to ZeuS. SpyEye is much more modular than ZeuS, and it makes the creation of additional plug-ins and extensions easier. There are many more plug-ins in SpyEye than in ZeuS to customize tasks, such as stealing credit card information. The extent of the infection, during week seven, was that about 2000 computers were infected.

Recognizing that this book is intended for an international audience, we have included an example of an infected log-in page stemming from an English-speaking bank rather than a Norwegian one. Figure 1.4 illustrates the proper log-in page, while the log-in page produced by the malware is shown in Fig. 1.5.

SpyZeus has configuration files for attacking specific countries and a user-friendly interface that is available in different languages. Still, the quality of the content of the configuration file does not seem to be fully developed. In the Norwegian version of the malware, there are a few eye-catching spelling mistakes and odd phrases. This weakness of the virus had been identified by many Norwegian customers who did not enter the fake site.

In the wake of a malware attack, we often see phishing attacks exploiting fear among the public that their IDs have been compromised. In the aftermath of the attack against the Norwegian banks, customers received e-mails purporting to be from their bank, in which the customer was asked to confirm log-in details, supposedly so that the bank would be able verify that the customer ID was not compromised. Of approximately one million recipients of phishing e-mails, only less than one hundred are reported to have submitted their authentication credentials. This fact is indicative of the vigilance and security awareness level of the public in Norway. The number of defrauded customers is very low, indicating that the public is highly security aware. This is an indication that the FIs have been successful in their attempt to educate their customers as to security risks that they face.

During log-in, the Trojan presents a false log-in page. When this happened, one bank had certain log entries posted to the bank's web-server log. The bank identified the signature of the log entry and developed an automated process that recognizes the signature, stops the log-in, and also automatically and instantly revokes the log-in credentials of the customer. Sharing this information allowed other banks to implement similar countermeasures. Analysis revealed that at the time of writing this, the Trojan is very context sensitive; i.e., a small change to the web of the Internet bank would fool the Trojan. This suggests that using random names for JavaScript functions and CSS class names would make the Trojan unable to recognize where to inject the malicious code and probably render the Trojan useless or less effective.

One important quality of a Trojan is its ability to hide itself. Encryption, hashing, and other techniques are being used for this. If the obfuscation techniques are elaborate, it takes resources and expertise to break them. Together the banks were able to "undress" the Trojan effectively. Once it was "undressed", the banks were able to devise effective countermeasures.

For more than 20 years, Norwegian banks have cooperated closely in the IT security area. Pooling resources, small and larger banks alike have developed resilient and uniform security systems enjoyed by all banks and their customers. Even though there are several different Internet banks being used, the system used for authenticating customers used by most Internet banks is jointly developed by the banks.

Banks exchange intelligence information related to IT security and together develop contingency solutions and emergency fixes. Once they were under attack, the banks swiftly convened under the auspices of a banking security organization; they were in day-to-day contact. In this way intelligence information was coordinated. Likewise, contact with other organizations, like the Norwegian National Security Authority (NSM), took place in a coordinated way.

This coordinated defense approach produced a number of countermeasures and other information that was shared between the banks.

An example of the coordinated defense approach is described here. The NSM discovered the attack. As the attack progressed, NSM sent regular updates containing more details on the progression and characteristics. It also notified banks and ISPs about which PCs had been infected. NSM did a comprehensive technical analysis of the specific malware (for example, a SpyEye-based attack) to be shared by all FIs. During this they discovered the IP of the command and control (C&C) center. By contacting the Norwegian ISPs, they were able to monitor the amount of traffic going from Norwegian customers to the C&C. In this way they got a picture of the severity of the attack, and also steps could be taken to close down the attack sites.

1.11 Information Sharing Against Cyber Crime in Italy

As far as cyber crime against the financial institutions is concerned, as we pointed out in the previous section, it is crucial to be able to quickly exchange updated information among the whole community of involved stakeholders. When a crime is committed against some financial target, the overall impact has to be analyzed on a chain of different players, ranging from service providers to mobile telecom operators, public institutions, law enforcement agencies (LEAs), payment systems, and end users, whose co-operation then becomes of paramount relevance to stop the consequent fraud, repress crime, and prevent its reappearance in the future. Two very good examples are represented nowadays by two initiatives realized in Italy, respectively led by the Italian Banking Association (ABI) and Poste Italiane.

1.11.1 Financial Institutions Information Sharing Working Group

The most important initiative specifically dedicated to creating a trusted community within the financial sector to exchange operative information about cyber crime, refers to a collaboration network promoted and run by the ABI, in the framework of its research and innovation center, ABI Lab. The network has been joined by more than 200 banks, Poste Italiane, the LEAs entitled to prevent and repress electronic crime (e.g., Polizia Postale e delle Comunicazioni), and the main telecommunications operators. Activities are steered by a Technical Committee consisting of the main ICT security teams in the Italian financial sector, coming from banks and service providers, who physically gather once every six weeks to monitor trends in cyber crime scenarios, share best practices, and plan initiatives to be implemented at the system level. The Technical Committee is chaired by ABI Lab, who leads the activities and is in charge of developing the community through specific tools and coordination of the offline communications among members. In this group framework, many actions have been realized so far, ranging from lobbying public institutions to raising customer awareness, from forming technical focus groups to defining guidelines for banks.

1.11.2 Presidio Internet

From an operative point of view, a sub-group has been created among the whole constituency regarding where to share information useful to counter cyber crime; it is called Presidio Internet. Presidio Internet is joined on a voluntary basis, and at the end of 2010 it was counting on more than 300 trusted peers, among banks, LEAs, centrally acknowledged by the Italian Banking Association through ABI Lab. Information is exchanged through a dedicated mailing list, where members define the confidentiality level to label the data they want to send and choose the security measures to eventually code the message. To this end, Pretty Good Privacy (PGP) keys are exchanged between members in case information needs to be encrypted. Governance of the information exchange is kept very simple, as unstructured data are also welcomed, and the ABI holds only a supervising role; it is not mandatorily asked to acknowledge if eventual messages are privately exchanged by two members. Still, the ABI plays the role of a third body, so it is possible to use it as a channel to anonymize information to be sent to the list. Each peer is asked to participate in the information exchange via a unique, highly recognizable interface, setting up a dedicated corporate e-mail address. Most importantly, members have agreed on the basic rule "*no obligation to share, nor to share everything*", which means that each one of them is allowed to choose how deeply to contribute to the information exchange. A crucial role to make things work effectively is played by the availability of LEAs to be part of an informal exchange of information. This allows members to be covered in case sensitive information must be communicated, as it would appear as a complaint filed to law enforcement.

ABI Lab continuously feeds the network with information from partnered info-providers, ICT security companies, specific mailing lists, international research centers, free alerting services, online resources, and European groups active in the field.

Information is exchanged on three different levels of confidentiality and can be addressed to one single member of the network, to a restricted sub-group, or to the whole constituency, either anonymously (via ABI Lab intermediation) or directly, as summarized in Fig. 1.6.

Operative information shared on the list refers to current threats and possible actions required of members, including informal requests for assistance to LEAs. Specifically, information shared on the list nowadays includes:

- malicious URLs, also sent to a blocking network and LEAs (approximately 100/week)
- stolen credentials recovered on malware drop zones (approximately 30 Mb/week)
- IP addresses from which fraud has been committed
- mobile telephone accounts used to charge credit from frauded credentials
- information regarding money mules activity
- phishing kits
- malware information from configuration files

Further, a monthly report to sketch trends, new threats, and possible countermeasures is produced and distributed to the whole constituency.

WARNING	Description	1-to-1	1-to-many	1-to-all	encryption
System Warning	Public information put together to point out an alert on ongoing threats potentially targeting the whole system		✓	✓	
General Warning	Public or private information which could have a direct impact on development of digital crimes throughout the system, with a low criticality	✓	✓	✓	✓
Specific Warning	Critical information on threats targeting one specific bank, coming from mostly private sources or LEAs, which require a real time reaction by that bank	✓			✓

Fig. 1.6 Information exchange in Presidio Internet

Last, with reference to contexts where information is collected, three initiatives worth mentioning have been started in Europe, with the aim of gathering expertise on the subject and proposing action plans to the relevant communitarian institutions:

- IT Fraud Working Group (European Banking Federation) is promoted by the European Banking Federation for sharing information on Internet fraud and discussing relevant initiatives activated by national banking associations.
- FI-ISAC Financial Institutions Information Sharing and Analysis Center (ENISA) is promoted by ENISA with the aim of focusing on all the issues related to electronic crimes, also through a dedicated mailing list. Constituency: banks, national banking associations, CERTs, and LEAs.
- ISSG/CISEG Cyber Crime Information Sharing Expert Group (European Payments Council) provides information sharing about cyber crime in the European community and defines formal documents supporting EPC initiatives in its definition of a roadmap to Single Euro Payments Area (SEPA).

1.11.3 Collaboration Between Banks and LEAs

Starting from the good experience and connections created in the framework of Presidio Internet activities, in 2010 a formal agreement was signed between the ABI and Polizia Postale e delle Comunicazioni, to make banks and LEAs share information on electronic crimes via a central database, owned and managed by the LEAs

themselves. Technical interfaces have been jointly defined and each bank is allowed to upload data and/or information relevant to investigation and analysis purposes. A format has also been defined to collect information on frauds that have already been committed as well as on potentially suspect operations. Thus the information flow is more structured than the one on Presidio Internet, and it is not allowed for the banks to communicate with each other, but each bank receives feedback from the LEAs and is warned if it is involved in some suspect operation. The benefits of this cooperation system are twofold. From a police perspective, having more structured data can help speed up an investigation process and provide more useful information on where to implement automatic intelligence and semantic analyses. From a banking system perspective, besides benefiting from a faster investigation, it is also possible to monitor the state of processing of the events, and each bank is able to access some aggregation of data, which is also useful in defining internal security policies.

1.11.4 The European Electronic Crime Task Force

The European Electronic Crime Task Force (EECTF) was founded in 2009 on the basis of a formal agreement between Poste Italiane, the United States Secret Services, and the Italian LEAs called Polizia Postale e delle Comunicazioni, who shared the mission to support the analysis and development of best practices against cyber crime in European countries through the creation of a strategic alliance between law enforcement, academic, legal, and private sector entities.

A governance model has been set up by the founding members, according to which an invitation to participate has been extended thereafter to the main stakeholders playing a lead role in countering cyber crime. Nowadays the EECTF is run via monthly meetings of permanent members, quarterly open events extended to a wide community of selected experts, and continuous sharing of relevant information within the whole community, also through dedicated specific tools.

The constituency of the EECTF is made up of founding members, permanent members, and a community of experts. Founding members are entitled to steer activities and define strategy, define policies for information sharing within and outside the community, define partnerships and decide new memberships, define outputs and dissemination strategies, and maintain the knowledge base. Permanent members are asked to actively participate in the community, with specific reference to share information according to a non-disclosure agreement, attend monthly expert group meetings, speak at quarterly plenary meetings, contribute to the growth of the knowledge base, propose new members, review and contribute to research outputs, and interact with each other via the members portal. The community of experts is continuously selected by EECTF founding members among LEAs, public institutions, banks and financial intermediaries, ICT, and a consultancy, and also from proposals made by permanent members. The community today has more than 200 members, who are invited to attend quarterly plenary meetings, are evaluated as a basis for potential new members, and who receive briefs of research outputs.

With the aim of collecting all of the available information and sharing best practices at an international level, the EECTF has been establishing international collaborations with some of the most relevant organizations, such as the European Network and Information Security Agency (ENISA), the Anti-Phishing Working Group, and the Digital Crimes Consortium. From a national point of view, links have been established with the Ministry of Economics and Finance and the Ministry of Internal Affairs, as well as the Italian Banking Association and the Information Sharing Working Group mentioned in the previous paragraph.

In order to make the most out of the competencies of the whole community of the EECTF, an Expert Group has been set up, which gathers on a monthly basis and is restricted to only founding and permanent members, with the aim of sharing highly technical information about new threats and possible countermeasures.

In order to identify trends and depict current scenarios, the EECTF has been carrying out yearly surveys on cyber crime in Europe by gathering reports, information, and analyses made by the key players in the field, including businesses, LEAs, and security intelligence experts at the international level. Key findings of the 2011 survey [14] point out characteristics of the cyber crime scenario, from both an operational point of view, sketching attack schemes and relevant countermeasures, and an organizational one, underlining a basic discrepancy between real threats and perceived risks, stressing the consequent need for a closer cooperation among the whole community of stakeholders.

A possible evolution at a strategic level of the EECTF depicts main goals on the medium term, which can be summed up in two directions: growth of community and growth of capabilities. If it is true that community grows on new memberships, it must also be considered that it grows above all with the increase of trust among members and the use of community tools, making it deeper and more reliable. The capabilities of the EECTF will grow together with the possibility to count on a wider knowledge base and on a plethora of specific competencies made available by each member.

1.12 Compliance to EU Regulation on Data Privacy

Financial institutions have to comply with several requirements as mandated for IT management and for data security. These standards identify three main security parameters: confidentiality, integrity, and availability. In this section we describe those regulations that are most relevant to information sharing and their implications for the deployment and use of collaborative platforms like the one presented in Part II of the book.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data, requires Member States to protect the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the community. The directive defines personal data as any information relating

to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications) translates the principles set out in Directive 95/46/EC into specific rules for the electronic communications sector.

Articles 5, 6, and 9 of Directive 2002/58/EC state the rules applicable to the processing by network and service providers of traffic and location data generated by using electronic communications services. Such data must be erased or made anonymous when no longer needed for the purpose of the transmission of communication, except for the data necessary for billing or interconnection payments. Subject to consent, certain data may be processed for marketing purposes and the provision of value added services.

Article 15(1) of Directive 2002/58/EC states the conditions under which Member States may restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3), and (4), and Article 9 of that directive. Any such restrictions must be necessary, appropriate, and proportionate within a democratic society for specific public order purposes, i.e., to safeguard national security (i.e., state security), defense, public security, or the prevention, investigation, detection, and prosecution of criminal offenses or of unauthorized use of the electronic communications system.

Under Article 8 of the European Convention for Protection of Human Rights and Fundamental Freedoms (ECHR), everyone has the right to respect for his private life and his correspondence. Public authorities may interfere with the exercise of that right only in accordance with the law and where necessary in a democratic society, inter alia, in the interests of national security or public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others.

Article 15(1) of Directive 2002/58/EC applies to data, including data relating to unsuccessful call attempts, the retention of which is not specifically required under this directive and therefore falls outside the scope thereof, and to retention for purposes including judicial purposes, other than those covered by this directive.

Article 30(1)(c) of Directive 95/46/EC requires the consultation of the Working Party on the Protection of Individuals with regard to the processing of Personal Data established under Article 29 of that directive.

Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems provides that the intentional illegal access to information systems, including the data retained therein, is to be made punishable as a criminal offense.

According to Article 23 of Directive 95/46/EC, any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with national provisions adopted pursuant to that directive is to receive compensation.

The 2001 Council of Europe Convention on Cybercrime and the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data also applies.

Articles 7 and 8 of the Charter of Fundamental Rights of the European Union defines citizens' fundamental right to respect for private life and communications and to the protection of their personal data.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks has been highly debated in many countries. Under much controversy and with a very slim margin, the directive was finally adopted by Norway on 4 March 2011.

Many EU countries have legislation on a national level covering data privacy. In Norway there is both a law and a regulation pertaining to protection of personal data. In line with the EU definition, personal data is defined as any data relating to one individual. Processing of personal data is defined as being any use of the information, e.g., collection, registration, compilation, storage and distribution or a combination of such. Personal data may be processed on the condition that the person has given her consent, or if the law paves the way for processing, or if operation on personal data is necessary in order to do the following:

1. to honor an agreement with the person, or to prepare for such an agreement,
2. for the operator to be able to fulfill a contractual obligation,
3. to defend the person's vital interests,
4. to perform a task of public interest,
5. to exercise public authority,
6. for the operator or a third party to whom the data is handed over, to maintain a valid interest, subject to the person's data privacy interests not being greater than said interest.

We conclude that the basic premise is that information relating to a person is to be kept private. Within the strict privacy rules of the current legislation, the question is then whether there is room for a collaborative system that collects, shares, correlates, distributes, and mixes and matches data. Under what conditions may such a system work?

Each person whose transaction data is to be received and processed by a collaborative platform would have to give her individual consent. Customer contracts would have to be amended to include provisions for data sharing, data protection, data processing, and data deletion. Any collaborative platform would have to guarantee that the data is maintained according to the provisions set out in the contract throughout the lifetime of the data.

The collaborative platform would have to maintain the data according to best practices when it comes to securing integrity, confidentiality, and availability. Data in transit would have to be end-to-end encrypted; i.e., the endpoints of the encryption tunnel would have to be either the data owner or a custodian approved by the data owner, the provider of the collaborative platform being one such custodian. Data at

rest should be encrypted. Access to data should be granted on a need basis, which means that there should be a hierarchy of encryption keys; one key giving access to limited amounts of data, and other keys granting access to larger data sets.

1.13 Concluding Remarks: Offline Collaborative Systems for Information Sharing

This chapter introduced the financial critical information infrastructure (CII) concept and the different types of stakeholders that may operate upon this specific communication infrastructure. Financial institutions and the communication network they use shall be considered one more type of CII to be protected, as well as other CII types such as the utility infrastructure and food supply chain. Nevertheless, financial CIIs have specific features and suffer different types of attacks than the other critical infrastructure types. The Norwegian CII has been described to exemplify required communication infrastructure characteristics and existing risks. Over the last 20 years financial CIIs have evolved according to new business models. The new communication channels that have been included at the edge of financial CIIs do not provide the same performance and security guarantees offered by traditional channels, thus creating vulnerabilities to cyber attacks. Transaction security is based upon software products to be installed at endpoints (such as VPN and crypto tools) and a set of process steps to be implemented by customers (such as an OTC-based identification process). It has opened the door to new challenges and new types of attacks that change their behavior over time, in turn starting a never-ending loop of implementation of countermeasures to face attacks that evolve over time, and thus requiring newly evolved countermeasures. Short descriptions of standard implemented countermeasures are provided. In this battlefield the financial stakeholders have discovered that coordination and information sharing may be strong weapons that reinforce all implemented countermeasures and speed up their deployment. Another important countermeasure relies upon information sharing with customers who are informed on how to reinforce their endpoints and on how they should react to threats. Some real-world cases exemplify the importance of information sharing. The creation of team experts to analyze threats is another way to react to threats. This is of special importance for viruses and malware that may be injected at any level of the CII, including endpoints. The expert team may "undress" the Trojans and identify antidotes to infection and procedures to neutralize the attack. This information may then be circulated to financial stakeholders in order to set up countermeasures.

However, the circulation of information and the corresponding analysis is done on a periodic basis that is too long, mainly through reports on mailing lists and physical meetings (such as Presidio Internet). This low frequency does not help in setting adequate countermeasures to attacks that take a very short time to be carried out. One of the most known collaborative systems for information sharing at the networking level is Dshield [6]. DShield could be seen as a world-wide sensor network

that collects data coming from the firewalls and the IDSs of volunteers. Currently, it covers 500,000 IP addresses over 50 countries. The data collected by the DShield system are sent to the Internet Storm Center, inserted in the central database, and analyzed offline by the staff of Internet Storm Center, called *handlers*, in order to detect spikes or malicious activities or evidence that an attack is taking place. This allows the creation of statistics about the most targeted ports, the top attackers, and the risk of worm outbreaks. A particular feature enabled for the active participants of Dshield is *fightback*, DShield forwards an authenticated mail to the ISPs of the identified attackers, which allows, in the case of massive attacks (such as DDoSs or Distributed Bruteforce), a quick response that can mitigate the attack. This system is based on a strong human component (the *handlers* of the Internet Storm Center). The team analyzes the records in the databases using aggregation tools, and if it finds evidence of a new attack it can alert the owners of the local sensors to ask for more data. If the attack is considered particularly dangerous, they can alert the core Internet backbone providers involved, and they may activate possible countermeasures. Apparently DShield does not enable sector-specific information sharing; it is focused on generic information sharing for networked ISPs.

To conclude, while the importance of information sharing is widely recognized, there is still no legal-technical framework that can manage sharing and correlation of events (possibly on the fly) among organizations that belong to the same market sector or that have specific market relationships (such as the financial sector). The implementation of such a framework could potentially reduce the time of threat detection and reaction by raising the level of awareness of any organization participating in the information sharing. Very often organizations from the same sector suffer very similar specialized attacks. Part II of this book is devoted to the description of one of these frameworks.

References

1. Financial Services Information Sharing and Analysis Center (FS-ISAC). Helping to protect the critical infrastructure of the United States. Available online at: http://www.fsisac.com/files/FS-ISAC_Overview_2007_04_10.pdf
2. US Presidential Decisional Directive (PDD-63). Available online at: http://www.fas.org/irp/offdocs/pdd/pdd-63.htm
3. The Role of Information Sharing and Analysis Centers (ISACs) in Private/Public Sector Critical Infrastructure Protection. Available online at: www.isaccouncil.org/whitepapers/files/ISAC_Role_in_CIP.pdf
4. Commission of the European Communities, On a European Programme for Critical Infrastructure Protection, Green Paper (2005)
5. Jackson, W.D.: Homeland security: banking and financial infrastructure continuity, CRS Report for Congress (2004)
6. Bologna, S., Setola, R.: The need to improve local self-awareness in CIP/CIIP. In: Proceedings of the First IEEE International Workshop on Critical Infrastructure Protection (IWCIP05) (2005)
7. Guard, M.B., Guard, L.M.: Physical and digital threats to financial institutions in the wake of the terrorist attacks. Available online at: http://www.bankersonline.com/security/cyberthreats.html

8. Basel II: Accord. Available online at: http://www.bis.org/bcbs/bcbscp3.htm
9. Basel II: Pillar One. Available online at: http://www.bis.org/bcbs/cp3part2.pdf
10. Basel II: Annex 9. Available online at: http://www.bis.org/bcbs/cp3annex.pdf
11. PCI Security Standard Council, Payment Card Industries (PCI): Data Security Standard Requirements and security assessment procedures. Available online at: https://www.pcisecuritystandards.org/security_standards/download.html?id=pci_dss_v1-2.pdf
12. Sommerville, I.: Software Engineering. Addison-Wesley, Reading (2001)
13. Federal Financial Institutions Examination Council (FFIEC): Information Security Booklet, Information Technology Examination Handbook (2006)
14. EECTF cyber cryme Survey (2011). http://www.poste.it/salastampa/CYBER_CRIME.pdf
15. www.elektroniskfaktura.com (2011)
16. Baldoni R.: Federated Identity Management systems in e-government: the case of Italy. Electron. Govern. Int. J. **1**, 64–84 (2012)

http://www.springer.com/978-3-642-20419-7

Collaborative Financial Infrastructure Protection
Tools, Abstractions, and Middleware
Baldoni, R.; Chockler, G. (Eds.)
2012, XXII, 226 p., Hardcover
ISBN: 978-3-642-20419-7