INFORMATION SECURITY IN BANKS AND FINANCIAL INSTITUTIONS
INFORMATION SECURITY THREAT SOURCES

Financial attacks mostly come from outside the institution, where intruders try to gain information or try to counterfeit the transactions. These institutions need to show their commitment toward reaching the highest level of security, and always staying up to date with the newest technique and technology.

Many cases have been reported as fraudulent, especially in fall 2012 in U.S., where the depository institutions were subject to denial-of-service (DDoS) attacks by a hacker group from Middle East. Another case was reported in the U.S., in 2014, where a major depository institution suffered data breach. Based on a public statement, the number of affected individuals and small businesses was 83 million. The institution declared that customer funds were not affected by this hacker group; however, the attackers managed to obtain customer information such as e-mail addresses, home addresses and telephone numbers.

According to GAO.GOV sources, another technique used to get access to customer funds and information is ATM Skimming, which costs depository institutions hundreds of millions of dollars annually. This technique involves placing an electronic device on an ATM machine to retrieve information from the card’s magnetic stripe at the time when a customer uses the machine.

THE IMPACT OF COMPROMISED INFORMATION IN FINANCIAL INSTITUTIONS

In general, data breaches lead to an abnormal high churn rate of the customer base. Additionally, in the financial industry, there will be investigations by the responsible regulatory bodies following a data breach, which could also lead to license termination for the affected organizations. Therefore, data breaches and security incidents require a rapid response to mitigate the impact on these institutions and to demonstrate due care. Banks and financial institutions need to strengthen their incident response teams to make sure appropriate encryption is used with all data, and also train their staff on a regular basis to acquire and maintain their BCM and DR capabilities, just to name the most efficient measures. To alleviate purely the financial impact of security threats, also insurance protection can be bought.

Depending on regulatory and legal obligations, organizational culture, geographic location and size, it might be appropriate to setup an internal or external CSIRT (Computer Security Incident Response Team). While the internal CSIRT is considered the most preferable option, businesses shy of the involved personnel costs could consider outsourcing these tasks to an external provider. On the other hand, a CSIRT is one of the most effective measures to cut data breach costs.
INFORMATION SECURITY IN BANKS AND FINANCIAL INSTITUTIONS

INSTITUTION AND EMPLOYEE RESPONSIBILITY TO ENSURE SECURE INFORMATION FLOW

Having software and tools available within an organization to safeguard information is not enough. Employees need to understand the threat’s effect in their working areas, and how crucial are the tools that must be used to defend against these threats. Thus, employee awareness and training is the key to resilience. They should always keep in mind that the information should be kept safe, and need to be vigilant not to become a victim of any counterfeiting actions.

Banks and financial institutions need to show their commitment to provide any necessary resources to ensure employees’ awareness. Among many criteria, there should also be a fulfillment of the following:

» The institution should implement a policy on how to govern its information security issues.
» Should have the authority and resources needed to carry out information security duties, including the implementation, maintenance and improvement of the information security management system.
» Institution should provide its staff with training and awareness sessions in order to understand information security policy and processes that are crucial for the institution.
» All employees need to be aware that passwords shall be strictly case sensitive and hard to be gained.
» There should be defined accountability on how to use the institution devices.

ONGOING STRATEGY TO KEEP INFORMATION SECURE

Retail banking and respondents from The economist and HP survey declared that banks and other financial institutions should pay more attention on securing information, rather than improving information flow.

The information security strategy needs to support the business objectives of the organization. Employing effectiveness and efficiency need to be improved in order to provide a better service for the customers. When performing security operations, a significant attention should be allocated to the necessary information that institution needs to provide to the employees, and this should be done appropriately and timely manner. Banks and financial institutions should be strongly committed on implementing a management system to deal with the security of information by employing people who are experienced and know how to deal with security issues.
Implementing ISMS based on ISO Standards is a massive assurance that an organization is meeting its regulatory requirements to apply due care to information security risks and that the ISMS is able to provide the whole organization with the necessary information. The ISO/IEC 27001 Information Security Management System standard ensures that organizations are addressing information security risks in a structured manner. Companies that obtain ISO/IEC 27001 certification validate that the security of financial information, intellectual property, employee details, or information entrusted from third parties is being managed successfully, and is improved continually according to the best practice approaches and framework.

PECB is a certification body for persons, management systems, and products on a wide range of international standards. As a global provider of training, examination, audit, and certification services, PECB offers its expertise on multiple fields, including ISO/IEC 27000 Information Security courses.

For further information, please visit: https://www.pecb.com/security-courses.

ABOUT THE AUTHORS:

Gezim Zeneli is an Account Manager for Information Security at PECB. He is in charge of conducting market research while developing and providing information related to Information Security Standards. If you have any questions, please do not hesitate to contact: marketing.sec@pecb.com.

Friedhelm Düsterhöft is a Senior IT Security Consultant and Managing Director of msdd.neT GmbH, offering ISO 27001 implementation, audit and training services. Please contact him at fd@msdd.net to discuss your specific needs and challenges. msdd.neT is an official PECB partner.