DeviceLock for compliance with GLBA & FACTA

Contents

Introduction

The protection of any personal consumer information stored in a financial company's information system is regulated in the US by two key laws: GLBS (the Gramm-Leach-Bliley Act of 1999) and FACTA (the Fair and Accurate Transactions Act of 2003). Both of these laws were drawn up in an effort to protect consumer financial information against leakage and abuse, and in order to prevent identity theft and other types of fraudulent behavior.

Under GLBA and FACTA, US supervisory bodies have prepared a number of special standards known as the Interagency Guidelines Establishing Information Security Standards ("Security Guidelines"). These standards clarify and provide the details for the requirements set out in GLBA and FACTA in terms of protecting sensitive client data. According to the Security Guidelines, financial organizations must undertake administrative, technical and physical security measures in order to guarantee the security, confidentiality, integrity and proper destruction of consumer information. The Security Guidelines came into force on 1 July 2005.

This white paper will review the requirements of GLBA and FACTA (Security Guidelines), which impact a company's information infrastructure and the security means used therein. This paper will also address the features of DeviceLock, a product by DeviceLock, Inc., which can help organizations achieve compliance with GLBA and FACTA much more effectively.

GLBA & FACTA Requirements

All companies which have any kind of connection to financial operations and consequently have access to consumer financial information fall within the scope of both GLBA and FACTA. This primarily concerns banks, insurance companies, brokerages, and transaction processing centers.

In particular, the requirements of the Security Guidelines regulate the storage and usage of sensitive financial data within companies, as well as the movement of these data between a variety of legal entities. Securing data when in moves outside a given company is of particularly concern today in light of the fact that consumer financial information is often bought and sold by banks, credit organizations, and insurance companies.

In order to minimize all possible risks related to the leakage and abuse of private financial information, the Security Guidelines require that security measures be taken during the storage and transmission of personal consumer information. In general, the key security requirements in the Security Guidelines pertaining to the protection of consumer information must be applied by financial organizations to ensure compliance with Section 501(b) of GLBA and Section 216 of FACTA.

The Security Guidelines stipulate that financial institutions must ensure the protection of consumer information regardless of whether or not a consumer is a client of the company in question.

Let us take a closer look at the term 'consumer information.' This term includes, for example, credit reports – a document category that typically contains a great deal of confidential information. A credit report could include information about an individual who applied for a loan but was denied, someone guaranteeing repayment of a loan, or information about an employee, or a potential employee. When entering into contractual relations, a financial institute must request that all of its service providers develop and implement the appropriate measures to ensure proper storage and use of this kind of information.

According to the definition provided in the Security Guidelines, consumer information includes any records which contain non-public, personal information about an individual who purchased a financial product or service from the company in question primarily for personal, family or family business purposes, and who has established long-term relations with the financial institution.

In order to protect consumer information, a financial company must develop and implement an information security program. This is a documented plan created in order to identify and control risks related to consumer information, and to ensure proper destruction of consumer information. The plan sets out policies and procedures for risk assessment, internal control mechanisms, testing, control over service providers, periodic audit and review of measures that have been taken, and reports to the board of directors.

The Information Security Program

Clauses II.A-B of the Security Guidelines require that a financial institution develop and implement an information security program which includes administrative, technical and physical security measures aimed at achieving the following goals:

- Guaranteeing the security and confidentiality of consumer information;
- Safeguarding consumer information against any foreseen threats or risks related to its security or integrity;
- Securing consumer information against unauthorized access and usage if the manifestation of said threats may result in considerable damage or considerable inconvenience to any consumer; and
- Guaranteeing the proper destruction of consumer information.

Implementing an information security program begins with performing an assessment of the most probable risks. Just as with other components of a security program, the procedures for risk assessment, threat analysis and all of the results thereof must be documented.

According to the Security Guidelines, risk assessment must include the following stages:

- Identification of the most probably internal and external threats which could lead to unauthorized disclosure (leakage), improper usage, distortion or destruction of consumer information or consumer information systems;
- Assessment of the probably and potential damages which may be caused by the identified risks, with due account for the level of sensitivity (confidentiality) of the consumer information;
- Evaluation of the adequacy of policies, procedures, consumer information security systems and other measures used to exercise control over identified risks; and
- Implementation of all of the stages described above with due account for the proper place and conditions for storing consumer information.

The standard's requirements include a list of security measures which must be reviewed by a financial institution and implemented as needed. The following security mechanisms are listed in Clause III.C.1.a-h of the Security Guidelines:

- Control over access rights to consumer information systems, including means of authentication and access rights exclusively for authorized users, as well as means of control over employee actions in order to prevent consumer information falling into the hands of unauthorized persons (which could result in fraud);

- Restricting access to the physical location of the consumer information, for example at the entrance to a building, information centers, record storage, etc. Only authorized persons should have access to these facilities.

- Encryption of consumer information in electronic format, including encryption during transmission and storage in networks and systems which may be accessed by unauthorized persons;

- Procedures guaranteeing that changes to consumer information systems will take place in compliance with the IT security program;

- Dual control procedures which delegate authorities to and run background checks on employees who have access rights to consumer information in line with their job descriptions;

- Monitoring systems and procedures which help identify actual attacks and attempted attacks against consumer information systems;

- Response programs which define actions to be taken if a financial institution confirms (or suspects) that an unauthorized person has gained access to consumer information systems, including filing a report with supervisory bodies and law enforcement; and

- Protective measures against the destruction, loss and damage of consumer information resulting from natural disasters and other dangers such as fire, flooding or technical difficulties.

In summary, the board of directors - or the appropriate committee - must take reasonable and prudent measures to ensure that an information security program is developed, implemented and maintained under the management of appointed employees. The board (or committee) must also approve the written information security program. Furthermore, according to Clause III.A, the board of directors must receive reports on program implementation and periodically review the results which have been achieved.

Meanwhile, management must report to the board (or committee) at least once per year, present the results achieved under the security program and confirm compliance with the Security Guidelines.

Clause III.F of the Guidelines states that the reports that management submits to the board must include information about the following: whether or not the financial organization assessed all relevant risks independently or engaged the services of an external consultant; whether or not agreements have been made with service providers; the results of testing; the identification of any bugs in the security system or breaches of policy; and finally, recommendations on adjusting the information security program.

DeviceLock from DeviceLock, Inc.

DeviceLock is endpoint device control software developed by DeviceLock, Inc. for corporate users. With DeviceLock, a company of any size can protect itself from the theft, leakage and corruption of information secured on corporate networks due to uploading and downloading activity via workstation ports, wireless networks or external drives. DeviceLock's key features include more than just control over local communications among computers based on assigned policies, it also provides complete shadow copying of all outgoing data. In contrast to the great number of solutions for the storage of email correspondence, DeviceLock facilitates the collection and analysis of data leaving the corporate network via workstation ports.

There is an ever-increasing number of mobile devices maintained and, in some cases, purchased by employees connecting to corporate networks. Experts at Yankee Group and SCS Research studied this trend toward the '*consumerization of corporate IT networks*' and advised IT department managers and directors neither to ignore nor to attempt to completely prohibit the plethora of portable devices used by employees. They simply must provide support for employees' mobile computers. Otherwise, the company risks losing its innovative and competitive edges by reducing the productivity of its employees. Meanwhile, mass consumerism is rife with new, serious risks in information security, as mobile devices may be used for fraudulent purposes, information leaks and other internal breaches. DeviceLock can help solve that problem.

When it comes to PDAs, smartphones and other communicators, DeviceLock does more than just support the shadow copying of all of the data exchanged to a mobile device - it also allows a company to apply flexible security policies and then track the enforcement of these policies. For example, DeviceLock may permit a user to synchronize his contacts and calendar, but prohibit copying files or synchronizing email with attachments.

DeviceLock also provides protection against hardware keyloggers, which are connected between a computer's keyboard and the system unit and used to steal valuable data from employee workstations. A malicious user can connect a keylogger between an employee's computer and keyboard, thus tricking antivirus software and other means of security. Once DeviceLock detects the exchange of data from the computer to the keylogger, it will warn the user and create a record in the events log.

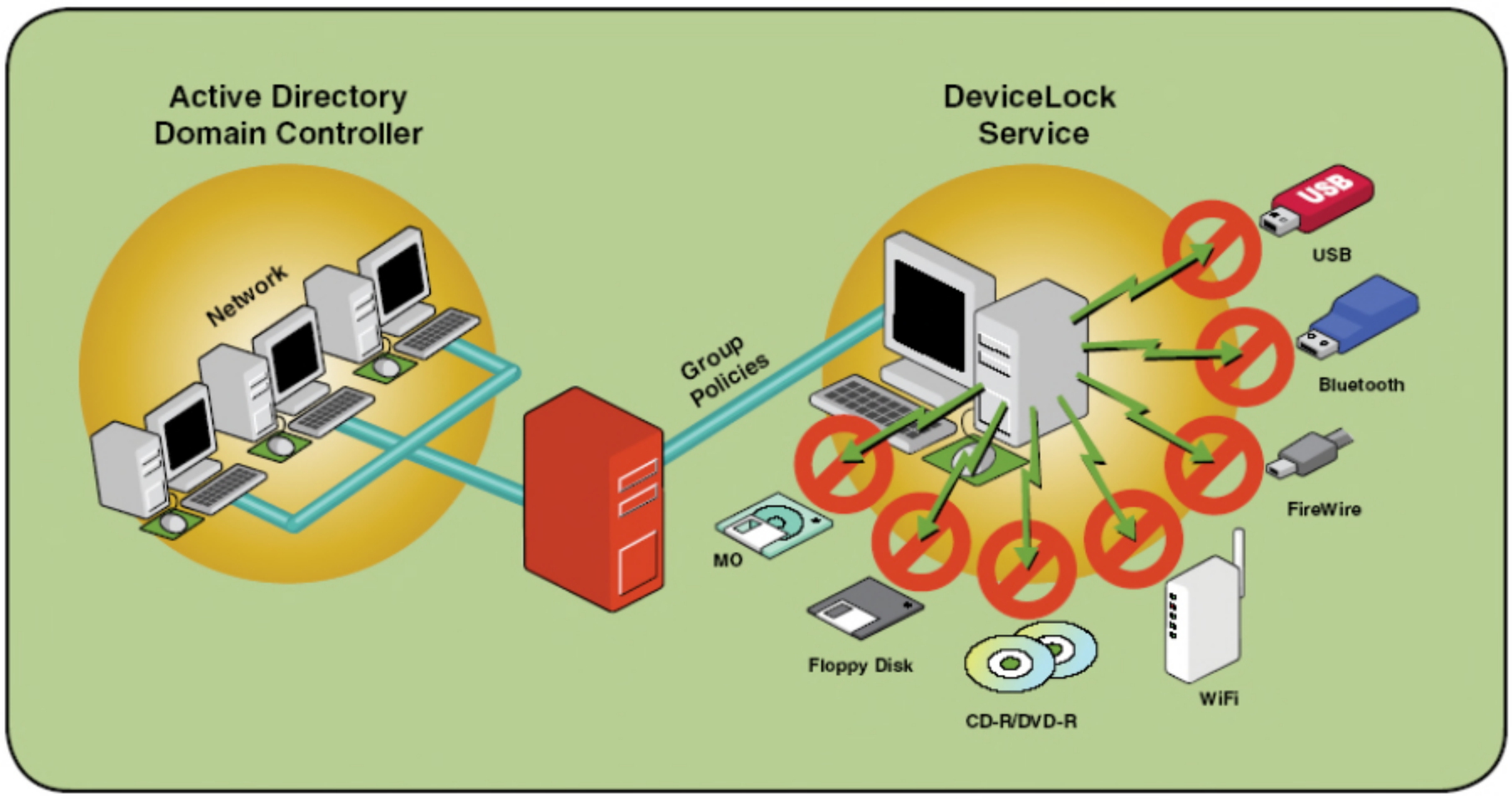
Through all these features, DeviceLock protects companies against the leakage of consumer information and other protected content, and serves as a tool for retrospective analysis of all data which company employees copy to external drives and take with them. It also affords a company the flexibility it needs in setting up information security policies when working with mobile devices.

DeviceLock consists of three parts: the agent, the server and the management console:

1. DeviceLock Service (the agent) is the core of DeviceLock. DeviceLock Service is installed on each client system, runs automatically, and provides device protection on the client machine while remaining invisible to that computer's local users.

2. DeviceLock Enterprise Server (the server) is the optional component for centralized collection and storage of the shadow data and audit logs. DeviceLock Enterprise Server uses MS SQL Server to store its data.

3. The management console is the control interface that systems administrators use to remotely manage each system that has DeviceLock Service. DeviceLock ships with three different management consoles: DeviceLock Management Console (the MMC snap-in), DeviceLock Enterprise Manager and DeviceLock Group Policy Manager (integrates into the Windows Group Policy Editor).



DeviceLock can be controlled using group policies in Windows Active Directory, making it easy to integrate it into the infrastructure of an organization of any size.

How DeviceLock Supports GLBA & FACTA Compliance

DeviceLock controls data movement via local workstation ports, wireless networks and removable drives based on flexible policies. Each time, the decision to either permit or prohibit access to an external device is made automatically. That means DeviceLock's settings and policies are easily audited, and DeviceLock itself does not create any additional information security risks.

Using DeviceLock in a corporate environment helps ensure compliance with the two key requirements of the GLBA and FACTA Security Guidelines:

- The Security Guidelines require that financial organizations exercise control over what employees do with personal consumer financial information (III.C.1.a-h). In other words, the company must ensure that information is protected against leakage and abuse. In this context, DeviceLock performs the functions of a necessary component of the internal control system, which can facilitate the management of access rights to local ports and interfaces and different types of data synchronization. The effective use of DeviceLock can significantly reduce the risk of uncontrolled data leakage and provides a way to record events in writing in the information security program.

- The Security Guidelines require that victims be informed in the event of leaked consumer information. In other words, a financial organization must have a mechanism in place to identify information leaks. Otherwise, the company may face large fines and have their license revoked. DeviceLock helps by shadow copying all data transferred to removable drives and mobile devices. By analyzing the information that the software collects, it becomes easy to identify where, when and how an information leak took place. Furthermore, an organization can find out exactly which files and records have been compromised. Pinpointing the leaked information can help speed notification of the individuals affected and avoid mass announcements to an entire client base.

The table below summarizes the features of DeviceLock and how they help support compliance with the GLBA and FACTA Security Guidelines.

Table 1. DeviceLock functions supporting GLBA and FACTA compliance

Requirements	DeviceLock Features
Development of a comprehensive information security program	A comprehensive program means that the company must take control over internal information security risks. This means it must minimize threats of leakage or abuse of consumer data posed by insiders. Using DeviceLock can help manage these risks, which gives financial companies a record of attempted violations of the security program and sufficient grounds for employee dismissal.
Identification of risks, assessment of threats and potential damages	Many companies try not to notice threats posed by insiders. Even so, ignoring the risk of a leakage or abuse of consumer financial information doesn't make much sense. The leakage of private consumer information can cost a company hundreds of thousand of dollars in direct losses, and multimillion dollar fines from regulatory bodies - not to mention a huge blow to the organization's reputation. DeviceLock can help solve that problem: inside violators will not be able to gain unauthorized access to workstations through their local interfaces in order to steal consumer data using removable drives or mobile devices. Meanwhile, DeviceLock's shadow copying features can provide evidence and documentation of both failed and successful attempts to gain access to and copy specific data.
Evaluating the adequacy of security policies and procedures	DeviceLock can help companies grant local access rights to information resources to just one employee, while blocking access to others. All authorities are delegated in line with the information security policy, the principle of minimum privileges, and common sense. This means companies can manage their internal security risks instead of ignoring them. DeviceLock will also create a much-needed database documenting the adequacy of internal procedures.
Access controls for sensitive information	One of DeviceLock's key features is the ability to both considerably lower the risk that sensitive information will be leaked by an authorized user, and keep a precise copy of all data which leaves the network via local workstation connections. That means a company can use DeviceLock to ensure it has control over all data that is copied from employee workstations.
Monitoring and identifying attacks	In order to find out whether or not an attack has been launched, a company should have an attack identification in place. DeviceLock's shadow copying function allows a company to keep tabs on whether or not an attack has been launched - and if one has, then the company will be able to see exactly which data have been compromised. Without this kind of system, a financial institution will not be able to identify a leak that was carried out using a removable drive or mobile devices; as a result, the company won't be able to notify the victim. In turn, this can lead to hefty fines and lawsuits.
Liability and reporting to the board of directors	The features of legislation similar to GLBA and FACTA are such that a board of directors may often be held liable for the effectiveness of the company's security program. DeviceLock helps significantly improve information support and the quality of reports issued by senior management and other company officers.

About DeviceLock, Inc.

DeviceLock, Inc. (formerly SmartLine Inc) was established in 1996 to provide effective and economical network management solutions to small, medium and large-scale business. Early on, we made it our mission to design software that is robust and reliable when it comes to enforcing network policy, while being easy and intuitive for system administrators to use. Furthermore, we made it our job to deliver solutions that are well-integrated and cost-effective. Based on this formula, we've introduced and developed category-leading products like DeviceLock for enforcing security policy related to personal devices.

DeviceLock, Inc. is a worldwide leader in endpoint device control security. Our DeviceLock product is currently installed on more than 3 million computers in more than 55 000 organizations around the world.

The company's customers include BAE SYSTEMS, AEROTEC Engineering GmbH, HSBC Bank, Barclays Bank, Chase Manhattan Bank, and various state and federal government agencies and departments.

DeviceLock, Inc. is an international organization with offices in San Ramon (California), London (UK), Ratingen (Germany), Moscow (Russia) and Milan (Italy).