

Financial Services: The Need for Visual Privacy

In the financial services industry, the protection of customer data and internal financial statements is non-negotiable. With rising customer security sensitivity, motivated attackers, and an increasingly complex legal and regulatory environment, data needs to be protected at all times – while it is stored, transmitted and viewed.

An important part of a comprehensive data protection strategy is ensuring visual privacy – the protection of data from people who may be able to view the screen of employees or customers. Visual privacy is often overlooked but it is a critical layer in protecting data from exposure. The need for visual privacy has increased substantially over the past few years. Consider the following:

- **A rise in the mobility of the workforce:** Driven by a blurring line between work/life and advances in mobile technologies, the mobility of workers has increased dramatically. IT analyst firm IDC estimates that over 72% of the US workforce has some level of mobility¹. By 2013 this number will increase to over 75%. Many of these workers will access corporate email/data in public areas through laptops and smart phones, putting that data at risk for exposure.
- **Requirements to report data disclosures:** Data breach notification laws have placed new requirements on corporations to notify customers if they reasonably believe that customer data was exposed to an unauthorized 3rd party. Currently, forty six states have breach notification laws². Businesses have long concentrated on exposure through the compromise of a database or the loss of data that is stored on a laptop or on storage media. Another avenue of data loss that must be considered and protected is identifiable information displayed on the screens of employees, like social security numbers and home addresses.
- **Ease of screen capture:** The ability of the average onlooker to capture information they view has increased substantially. According to a recent survey, over 60% of US households now have at least one camera phone³. This means that most users have the ability to capture images, including screens shots, which increases the threat from snoopers.

Any *defense-in-depth* approach to safeguard data must include protecting that data while it is displayed on a screen. Visual privacy is critical to both protect information and to build a case of “due care” for auditors and regulators. A comprehensive protection strategy has to address the entire data lifecycle: entry, transmission, storage, use, display and disposal.

¹ IDC Worldwide Mobile Worker Population 2009–2013 Forecast,

<http://www.idc.com/getdoc.jsp?containerId=221309>

² National Conference of State Legislatures,

<http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx>

³ PMA Marketing Research, <http://pmanewline.com/2010/03/15/pma-data-watch-camera-phone-penetration-continues-to-rise/>

Privacy and Compliance in Financial Institutions: An Overview

Financial services organizations have seen a rise in regulatory and compliance standards around customer and corporate data. While controls may be in place to defend this information as it is stored and transmitted, security is equally important for data as it is entered, processed, and viewed. Some important laws/standards to consider are:

Gramm-Leach-Bliley Act (GLBA):

The GLBA, signed into law in 1999, requires financial institutions to define a privacy policy for customer data and to put reasonable safeguards in place to protect that data. At some point much of this data will be displayed on employee screens.

Breach notification laws:

Currently, 46 states require that a customer be notified if a company suspects that his/her personally identifiable information (PII) has been exposed to an unauthorized 3rd party.

Payment Card Industry Data Security Standard (PCI DSS):

Defines procedures for keeping payment card information secure. The PCI DSS is under constant revision and is being adapted to cover a wide range of threats.

Other standards/laws: Other laws and standards such as ISO 27001, ISO 27002, and Sarbanes Oxley have direct implications for data confidentiality. In practice, the litmus test of “due care” is being recalibrated to include protection beyond data storage and transmission.

The information security industry has long recognized the importance of visual privacy. For example, passwords are typically masked as they are entered into an application or website. This need has been specifically called out for financial services. The Federal Trade Commission guidelines for complying with Gramm-Leach-Bliley Act (GLBA) require “using password-activated screen savers to lock employee computers after a period of inactivity.” For Financial Services organizations the range of sensitive data that is entered, processed and viewed goes far beyond passwords and steps must be taken to protect that data from opportunistic observers.

The GLBA specifically calls out the need for “administrative, technical, and physical safeguards” to keep customer financial data safe from exposure to unauthorized 3rd parties⁴. Some companies have tried angling cubes/monitors in public areas or isolating computers that will have sensitive information to try to keep visual data safe. A privacy filter gives organizations more flexibility to place workers where they want and need to be, maximizing productivity. Privacy filters go further in that they help protect data from individuals who might enter what is considered a protected space.

3M, a leader in this category, offers a range of privacy filters which effectively block out side views, help reduce the risk of data exposure and protect an organization’s most valuable resource: its data. 3M Privacy Filters come in a range of sizes and styles to protect laptops, desktops and even mobile phones. For more information visit: <http://www.3Mprivacyfilter.com>.

⁴ Gramm Leach Bliley Act of 1999, <http://www.ftc.gov/privacy/glbact/glbsub1.htm>