

Secure Office Systems for Privacy Compliance



Data and Network Security for
Financial & Banking Applications



Privacy Legislation Drives the Demand for Secure Office Systems

Financial Market  Gramm-Leach-Bliley

Healthcare Market  HIPAA

Both acts contain privacy and security provisions





What is Gramm Leach Bliley?

- The GLB Act applies to “financial institutions” designed to protect information collected about individuals
- The enforcement is performed by government agencies
- The FTC Safeguard Rule implements the security provisions of the Gramm-Leach-Bliley Act of 1999
- Took Effect May 23,2003, with an extra year to conform third-party service provider contracts entered into prior to June 24, 2003





What information is covered?

- “Customer information,” which means:
 - Nonpublic personal information concerning the financial institution’s own customers; and
 - Nonpublic personal information that receives from a financial institution about customers of another financial institution;
- Note: Customer information includes information handled by affiliates





Affected Organizations

- Banks / Lenders
- Credit Card Issuers
- Mortgage/ Title
- Brokers/ Stock Trading Companies
- Financial Advisors/ Tax Preparers
- Services Affiliates
 - Check processors
 - Collections





Standards for SafeGuards

- Each Financial institution must develop, implement and maintain a comprehensive information security program that is written in readily accessible part(s)
- The program must contain administrative, technical, and physical safeguard that are appropriate to:
 - The size and complexity of the financial institution
 - The nature and scope of its activities;
 - The sensitivity of its customer information



Each Financial Institution must:

- Designate one or more employees to coordinate its program
- Assess risks to security of customer information
- Design and implement safeguards to address these risks, and test and monitor their effectiveness over time
- Oversee service providers





Areas of Operation

- To assess risks and design safeguards, a financial institution must consider all relevant areas of operation, including:
 - Employee training and management
 - Information systems, including network and software design, as well as information processing, storage, transmission and disposal
 - Detection, prevention and response to attacks, intrusions, or other system failures





The Risk to Privacy Compliance

Digital Copiers Store
Thousands of Records

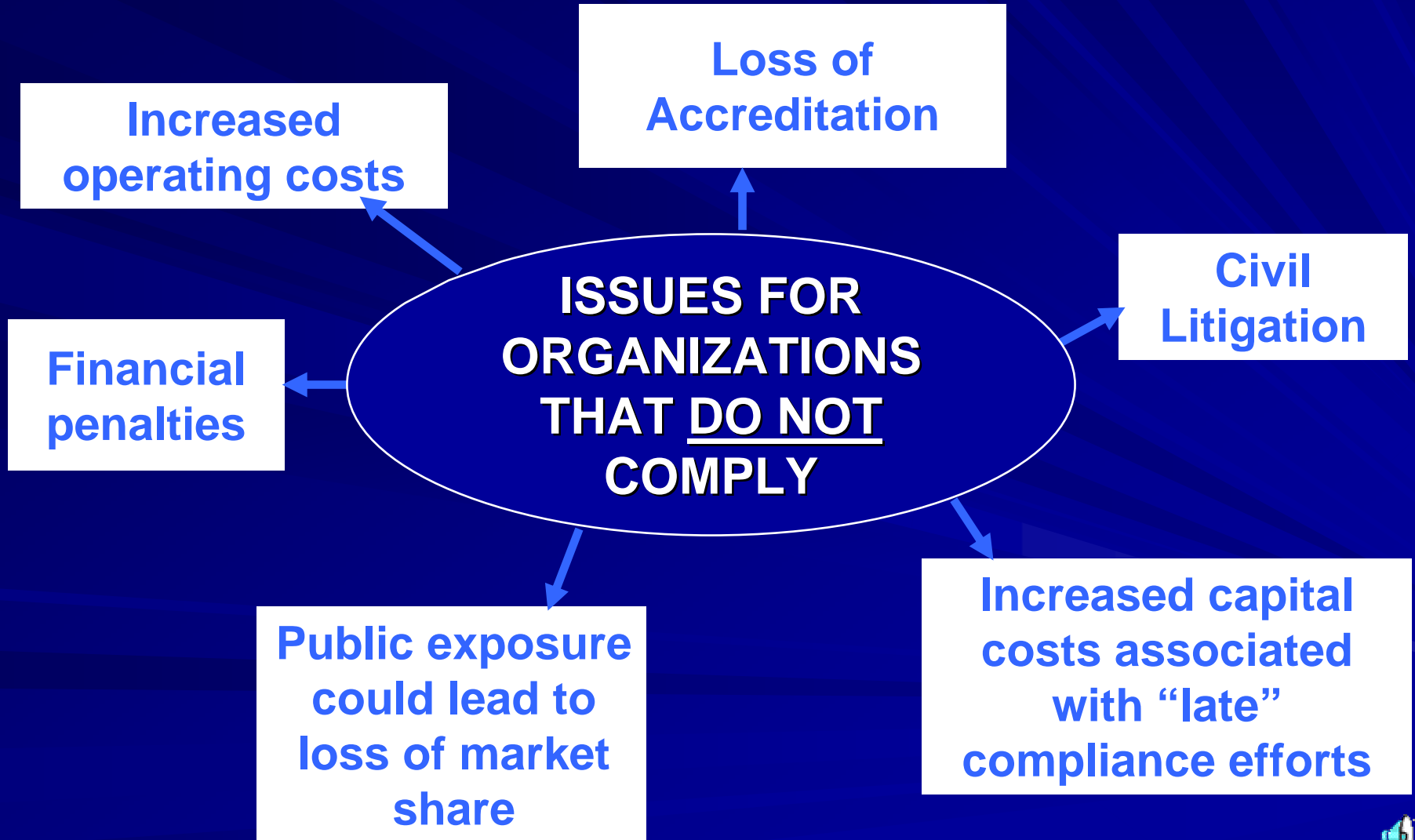


At the end of a copier's lease period, thousands of records retained on the hard drive can fall into the wrong hands...this poses a privacy compliance risk





Associated Issues of Non-Compliance





Privacy Conformance Steps

- ✓ ■ Appoint a Privacy Officer
- ✓ ■ Perform a Gap Analysis
- ✓ ■ Modify Contracts
- ✓ ■ Design Forms
- ✓ ■ Develop Policies & Procedures
- ✓ ■ Institute a Training Program
- Implement a Secure IT Infrastructure...*including your office equipment*





GLB Offers Opportunity for Secure MFPs

- The Financial/Banking Market
 - Is mandated to change
 - The implementation process has started
 - Privacy Violations can be fined NOW
 - The threats of civil lawsuits are even more pressing
 - Customers are receptive to help
 - HDD/Memory Exposure could be serious





SHARP Security Solution

Electronic Data Disclosure Prevention

Copy/Print Data

John Smith
SS#
Diagnosis



Gr752#47
&j@#
3N%\$?*

[Blank document icon]

Data is erased every time copy/print job is completed. "Clear all memory" mode enables MFP to erase all data area when MFP is turned on.

Encryption

Data Clear



HDD



HDD, RAM, FAX Flash memory are erased



Volatile Memory





Common Criteria Validated Data Security Kit

■ What is the Importance of Common Criteria?

- Security claims validated by the National Security Agency
- Difficult to attain
- Sharp is on its **Second Generation**
- Proven success in government/military applications

■ Data Encryption

- 128 bit encryption
- Hard Drive, RAM or ROM for print, copy, scan, or fax

■ Data Overwrite

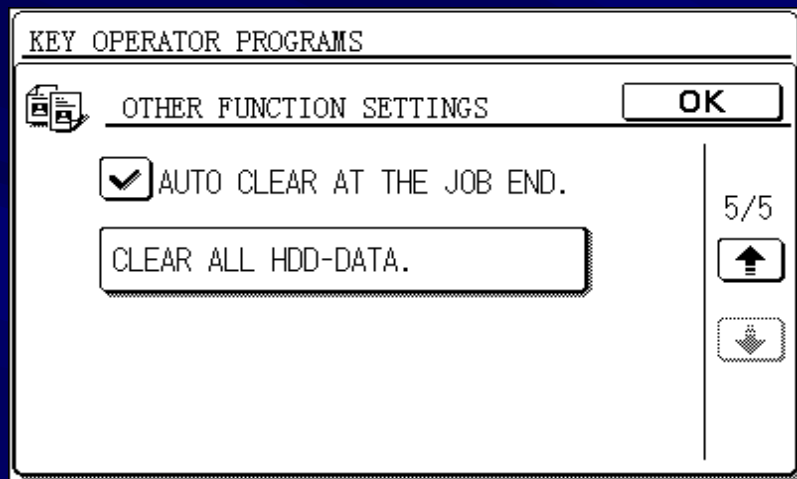
- Random numbers overwrite (up to **Seven Times**) the information written to memory when a document is printed, copied, scanned or faxed
- Hard disk overwrite for print, copy and scan functions
- RAM overwrite for print, copy and scan functions





User Notification

Manual Mode



Message displayed at the completion of each job indication that the memory has been cleared

Auto Mode





Sharp offers “End-to-End” Security

■ Confidential Printing

- Print is made while author is present
- Minimizes the risk of secure documents being removed from the paper tray

■ Audit Trail

- Allows network administrators to monitor all print, copy and scan activity
- Provides a comprehensive audit trail that can track network activity by user
- Tracks every page that is printed and copied





Sharp offers “End-to-End” Security

■ Secure Network Interface

- MFPs have network-accessible web administration pages
- IP Filtering and MAC Address Filtering allow administrators to restrict user access, disable protocols and disable ports





Who's Involved in the Decision Process

Key Messages:

Security technology
Privacy Compliance



- Privacy Security Officer
- Compliance Administrator

HP Compatibility
System Compatibility



- IT Manager

Equipment/Operation
Cost
Service Response



- Purchasing





Sales Approach & Discussion

- Arrange a meeting with the key decision makers *including the Privacy Officer*
- Create awareness of the current risks
 - Current digital copiers are not secure
 - Digital Printers have the same issue
 - Costs per page are lower with Sharp
 - Networked machines are at risk from hackers
- Discuss the secure feature set of IMAGER™ models
Install a Trial Unit including:
 - Data Security Kit
 - Secure Network Interface Card (insure the correct configuration)

