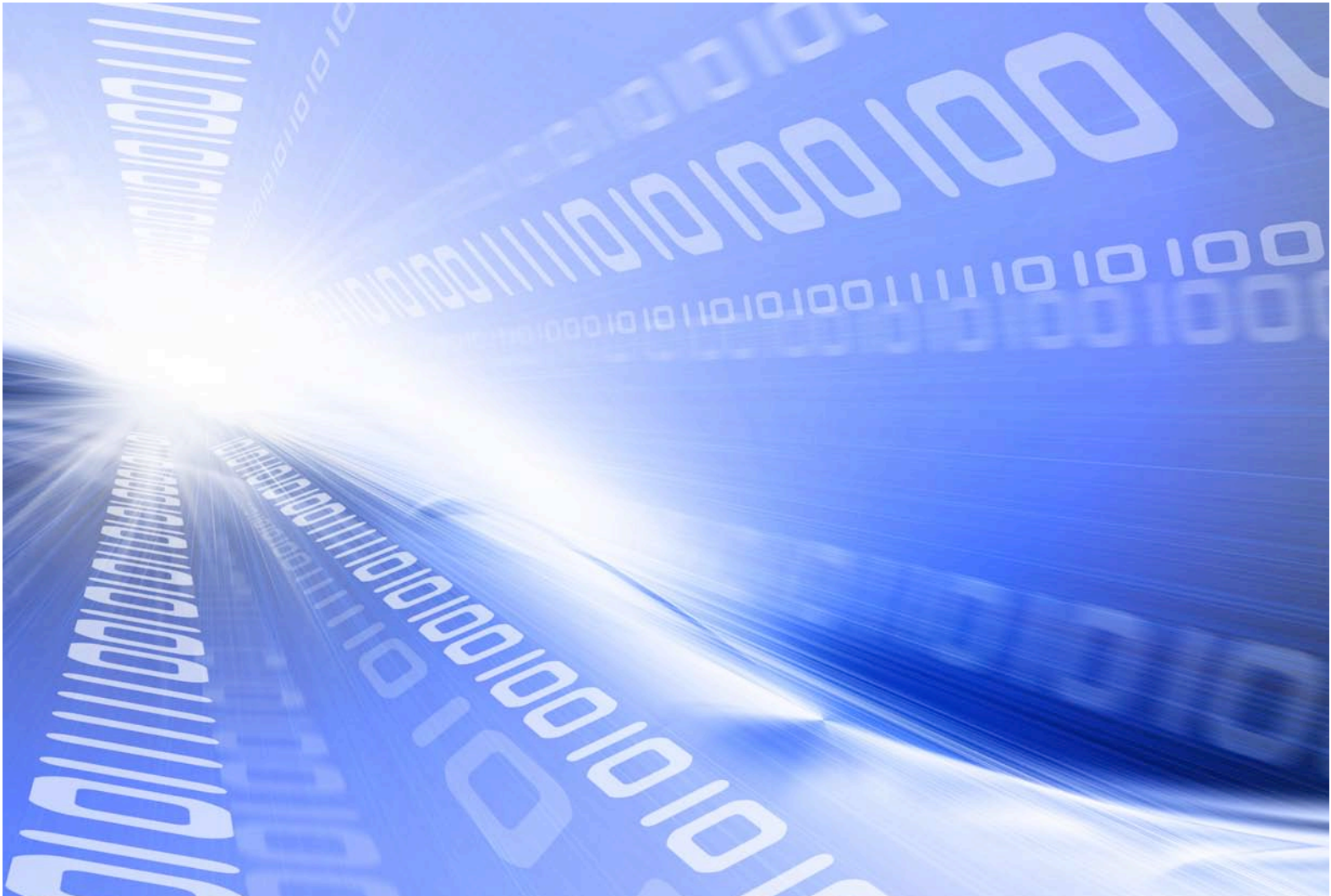


Regulatory Compliance and MFP Security Solutions

Key Issues and Considerations

A Muratec Whitepaper
2009



DEPLOY. DUPLICATE. DIGITIZE. DELIVER.

muratec

(This page intentionally left blank)

Table of Contents

INTRODUCTION	4
WHAT IS INFORMATION SECURITY?	4
Threats to Information Security: High-profile Cases	4
Insider or Outsider?.....	5
The Impact	5
WHAT IS REGULATORY COMPLIANCE?	6
Common Regulations	6
GLBA.....	6
HIPAA.....	6
SOX.....	6
FERPA	6
TARGETED SECTORS, AT-RISK INFORMATION	7
Questions to Ask.....	7
SECURING THE WORKFLOW	8
Input Solutions.....	8
Process Solutions.....	8
Output Solutions.....	9
CONCLUSION	9

INTRODUCTION

In the early 1980s securing a computer, printer or fax machine meant placing it behind a locked door. That was before computers were on every desktop, and before the advent of multi-functional products (MFPs). The MFP consolidates functionality into a single, space-saving platform, enabled businesses to address varied document processing needs, specifically walk-up copy and fax operations and network scan, fax and print functions. From document creation through output and distribution, the MFP plays a pivotal role in today's connected workplace.

Indeed, as a centralized document processing hub, the MFP has transformed the office landscape by speeding the generation and dissemination of information. In the pre-Internet era documents were carried by courier or express mail services. Now those same documents are easily converted into electronic files, via the MFP, and communicated locally or globally—in an instant. As technology has evolved, so too has the speed at which business moves.

This shift from paper-based to electronic business processes presents formidable challenges for IT security professionals, and others tasked with safeguarding information assets. With nearly instantaneous dissemination capabilities, business-critical documents can be routed to unauthorized individuals in seconds.

To remain competitive in today's challenging economic climate, organizations—now more than ever— have to protect information assets from theft or loss. Information security is particularly critical for businesses subject to a labyrinth of federal regulations, such as HIPAA, SOX and GLBA. In this white paper, we will examine the issue of regulatory compliance as it relates to office technology, and thus provide guidance on security solutions that can help support enterprise-wide compliance initiatives.

WHAT IS INFORMATION SECURITY?

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. The terms “information security” and “information assurance” are often used interchangeably, but have the same meaning—to protect the confidentiality, integrity and availability of information.

Confidentiality is the cornerstone of information security, and is defined by the International Organization for Standardization (ISO) as “ensuring that information is accessible only to those authorized to have access.” Integrity is the assurance that data is consistent and correct. Availability means that the computing systems and security controls, used to process and protect the information, respectively, are available and functioning when the information is needed.

Threats to Information Security: High-profile Cases

Theft of intellectual property, trade secrets, personal financial information and medical records is not uncommon, as illustrated by a 2006 incident involving a security breach at Coca-Cola. An administrative assistant stole confidential documents, possibly even the closely-guarded Coke formula, and attempted to sell the information to Pepsi. Pepsi contacted Coca-Cola, who in turn contacted the FBI.

Even the FBI is not immune to moles. Robert Hannsen, a former FBI agent serving a life sentence in solitary confinement, carried reams of classified documents containing highly-sensitive security information out of FBI headquarters. Hannsen was charged with selling American secrets to the Russian KGB for more than \$1.4 million in cash and diamonds over a 22-year period.

Other high profile cases, where confidentiality, integrity and availability of information was compromised, with disastrous consequences, include Enron, Tyco and WorldCom. In those cases, e-mail and paper documents were destroyed, in an attempt to thwart investigators. And though legislation has been enacted following those scandals, people that seek financial gain will continue to surface, as we've witnessed with the massive \$50 billion Ponzi scheme perpetrated by Bernard Madoff. The world-wide economic impact from the collapse of these enterprises, and countless others, has cost public and private businesses, charities and individual investors billions of dollars.

Insider or Outsider?

What these breaches in security demonstrate: 1) greed is alive and well, 2) the greatest threat to information security originates from within. In fact, software and services provider Compuware found that data breaches at companies are caused by staff in 75 percent of cases, compared to just 1 percent by outside hackers. Backing up those findings was a survey, "Trends in Proprietary Information Loss," sponsored by the National Counterintelligence Executive & ASIS Foundation. This study found that the primary risk to information assets included:

- Deliberate (and inadvertent) actions of current and former employees.
- Exploitation of trusted relationships with vendors, customers, joint ventures, partners, and subcontractors/outsourced providers.
- Data mining and software driven collection of open-source data and public information.



The Impact

Clearly, there's a broad spectrum of activity that can qualify as a threat to information security. In terms of office technology, a negligent employee in a doctor's office could accidentally fax test results to the wrong destination. Or a disgruntled hospital employee could copy a celebrity's autopsy report and sell it to a tabloid. Whether the breach is accidental or intentional, the damage could mean...

- Costly litigation
- Fines and imprisonment
- Erosion in public trust/reputation
- Diminished competitive advantage
- Loss of shareholder confidence
- Reduced revenue stream
- Embarrassment

WHAT IS REGULATORY COMPLIANCE?

Based on the serious ramifications of lax information security it's no surprise that the federal government has stepped in. Far-reaching legislation has been crafted to protect not only the integrity of information and data, but also to require the implementation of administrative best practices.

Consequently, corporate, public and private agencies are tasked with addressing rigorous compliance mandates, creating an industry unto itself—regulatory compliance. Regulatory compliance means putting in place policies and procedures that ensure personnel are aware of and take necessary steps to comply with relevant laws and regulations.

Common Regulations

While the details of federal regulations can fill volumes, the following are frequently cited when the topic of regulatory compliance arises:

- **Gramm-Leach-Bliley Act (GLBA)** is a 1999 federal law that governs the collection and disclosure of personal financial information. For example, insurance companies are required by this law to provide a yearly notice to customers describing how they will treat their customers' personal financial information. Under GLBA, CEOs and directors can be held personally accountable for any misuse of personally identifiable information.
- **Health Insurance Portability and Accountability Act (HIPAA)** legislation was enacted by the U.S. Congress in 1996. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA includes The Privacy Rule, which governs use and disclosure of protected health information (PHI) and The Security Rule, where administrative, physical and technical safeguards are outlined.
- **Sarbanes-Oxley Act (SOX)** legislation was passed in 2002 in the wake of the Enron scandals. Affecting all publicly-traded corporations, SOX governs accounting and disclosure of financial information, including provisions for documenting internal controls and procedures for financial reporting. SOX requires that management take responsibility for the integrity of financial information, i.e., evaluate IT systems and processes and produce evidence that the company has done a reasonable job keeping sensitive information safe.
- **Federal Education Rights Privacy Act (FERPA)** of 1974 is a federal law that protects the privacy of student education records. This regulation provides that educational agencies and institutions that receive funding under a program administered by the U. S. Department of Education must provide students with access to their education records, an opportunity to seek to have the records amended, and some control over the disclosure of information from the records.



TARGETED SECTORS, AT-RISK INFORMATION

Heavily regulated sectors include healthcare, financial services and education. Other sectors not listed below, yet still subject to government regulation are utility, automotive, pharmaceutical and retail. These and many other sectors share a common goal: Ensure that high-value information is handled in accordance with company policies and procedures.

Sector	Regulation(s)	At-risk Information
Healthcare (hospitals, pharmaceutical companies)	HIPPA	<ul style="list-style-type: none"> Protected health information
Financial Services (banking, insurance, securities)	GLBA, SOX	<ul style="list-style-type: none"> Credit history Stock buy/sell orders Insurance claims Financial statements Foreclosure records
Education (primary & secondary schools, colleges, universities)	FERPA	<ul style="list-style-type: none"> Student educational records Test data

Again, this is just a sample of regulated sectors, as there are dozens of major industry classifications and regulations that apply to each. Furthermore, some sectors will overlap in terms of at-risk information and applicable regulations. For instance, a university's on-campus student health center handles patient information, thus is subject to both FERPA and HIPAA regulations.

Within hospitals, insurance companies, brokerage firms and universities a chief compliance officer (CCO) is typically responsible for overseeing and managing compliance issues, ensuring that personnel are complying with regulatory requirements, as well as internal policies and procedures. The role of CCO is federally mandated for publicly-traded companies that are subject to SOX regulations, as well as broker-dealers and registered investment firms. Other sectors have also created CCO positions in response to the aforementioned scandals.

Another key position in larger enterprises is that of chief information security officer (CISO). As the title implies, the CISO's job focuses on information security within an organization. The job's responsibilities vary but often include development of security statements, mandates, governance, policy, training and awareness.

Questions to Ask

Though much has been written on security solutions that assist with compliance, meeting stringent mandates is a daunting task. To make that process easier, we are providing guidance about core security solutions supported by the Muratec line of workgroup MFPs, facsimile systems and associated software applications.

Before reviewing these solutions, however, there are some key questions to ask; the answers will help focus the discussion and, perhaps assist in the selection of Muratec technologies that will best address potential vulnerabilities.

- What is currently being done to secure network peripherals?
- What are the most valuable information assets—sales forecasts, client lists, secret formulas, R&D data, policy data, computer source code, medical records?

- What percentage of information assets are in paper form? In electronic form?
- Would directing incoming fax messages to e-mail be preferable to hardcopy reception?
- Do users on the network have to sort through print jobs to locate their own document(s)?
- Do fax messages sit on the output tray for passersby to see?
- For auditing purposes, would archival of inbound and outbound faxes be important?

SECURING THE WORKFLOW

Using the document workflow concept – Input > Process > Output, there are specific Muratec security solutions that can protect information, and at the same time make individuals cognizant of their role in maintaining security. Implementation of all these features is not practical, nor necessary, only those that meet corporate-wide or departmental information security objectives.

For instance, requiring a user to authenticate at the device may be a minimum IT requirement. In others cases a multi-layer approach may be necessary to control not just physical access to device functions but how the system processes, retains and archives documents and data. This involves understanding and managing risks in a way that is scalable to the environment.

Input Solutions

NTLM Authentication – Restricts access to the device by requiring a user to enter his/her domain user name and password. When authenticating over the network, subsequent scans to e-mail/FTP/folder are encrypted using the Kerberos standard from RSA®.

Personal Address Book – Users can be assigned their own password-protected contact list containing private fax numbers, e-mail addresses and/or folder structures. In financial sectors, for example, protecting client privacy is a priority.

Password-protected PDF – If interception and viewing of sensitive documents is a concern, the document can be scanned as a password-protected PDF. Only those that know the password can open/view the file.



Process Solutions

Fax Routing – To prevent incoming fax messages from printing out for all to see, messages can be routed to the intended recipient's e-mail inbox or network folder. Besides assisting with privacy regulations, this feature provides today's mobile workforce with anytime, anywhere access.

Fax Archival – All inbound and outbound fax and e-mail transmissions can be archived to a network location, creating an audit trail that meets regulatory compliance needs.

Fax Forwarding – To protect the confidentiality of fax-based communications, inbound fax messages can be forwarded to another remote fax. When traveling to the branch office, for instance, sensitive or urgent fax messages can follow.

Output Solutions

Print on Demand – From the machine’s touch screen, users can retrieve frequently produced documents from a secure network folder, eliminating the need or concern over displaying and printing documents from a desktop computer.

Secure Print – Requires that the user enter his/her user ID and password (at the control panel) in order to release the print job. Output can’t be viewed or picked up by the wrong person; no need to sift through multiple pages, enhancing productivity.

Secure Fax Reception – In non-networked environments, for instance, incoming fax messages can be stored in the machine’s internal memory, and printed upon entry of a valid passcode; ensures that only authorized parties access the information.



CONCLUSION

Valuable network resources are protected by firewalls, anti-virus software and ongoing security testing for holes and break-ins, but the MFP—a vital network on-/off-ramp—is often overlooked. With that said, steps can be taken to leverage Muratec’s robust security technologies to enhance information security, and at the same time address enterprise-wide compliance initiatives. While no security solution can guarantee protection against all threats, exercising due diligence in the selection and implementation of appropriate countermeasures is a fundamental first step.

###