# HP Imaging and Printing Security Best Practices

Technology for better business outcomes

# HP imaging and printing security strategies mitigate risk

As imaging and printing products become more tightly integrated into critical business operations, the capabilities enabled by these printing systems can create additional security risks. Unsecured printers, or any product that resides on the printing network, can cause a costly security breach if private information is jeopardized. A secure business environment comes from having a clear understanding of legal requirements, knowing how your imaging and printing infrastructure maps to those requirements and understanding the usage patterns of your employees.

According to a 2008 Forrester Research survey of 364 executives at North American and European enterprises, enterprise customers plan to spend 8% of their IT budgets on IT security.

*Enterprise IT Security Budgets, Q4 2007, Forrester Research, January 3, 2008*

## Is your company at risk?

The costs of exposing sensitive documents, such as compromised public security, stolen intellectual property, revealed marketing plans, and confidential customer lists, are potentially devastating. And it's not always external threats that pose risks to your organization.

Recently, an investment bank employee leveraged confidential information about impending deals from documents left on a nearby, unsecured printer. The result: $7 million in ill-gotten gains, litigation and negative publicity for the firm.

HP has identified six principle threats:

1. **Hard copy** – confidential documents that are left lying on the printer output tray for anyone to see
2. **Network sniffing** – illicit "sniffs" to print data from the network can provide anyone with a copy of a printed document
3. **Theft** – someone stealing either the printer or the printer hard disk to obtain vital information stored inside
4. **Product configuration** – unprotected products can be reconfigured, under certain conditions, to divert print jobs and expose confidential information
5. **Information disclosure** – multifunction printers (MFPs) and digital senders can be used to send confidential documents via e-mail or fax, which bypass security control mechanisms
6. **Network penetration** – malicious software can be installed in modern printers to spy on information within the network

## What are other companies doing about it?

More than 70 percent of Fortune 1,000 companies in the U.S. are increasing their security budgets to meet regulatory and audit compliance requirements, such as Sarbanes-Oxley and the Payment Card Industry data security standard.[1] Not a bad idea, considering that the Privacy Rights Clearinghouse reported more than 100 million personal records have been improperly exposed from 2005 through 2006.[2]

## The HP security framework for imaging and printing

HP offers a wide array of imaging and printing security solutions. Our strategy tackles the imaging and printing products, the network, and the data passing across the network. It can be broken down into the following key areas:

1. **Secure the product** – HP offers secure imaging and printing products designed to prevent unauthorized users from accessing confidential information in the printer or its output tray, or changing the product's configuration.

   The HP Access Control Secure Printing solution requires authentication at the printer before a print job is released. HP also works closely with its solution partners to provide a wide variety of authentication methods and pull printing capabilities.

2. **Protect information on the network** – The HP JetDirect product family provides network connectivity for HP printing and copying products. HP JetDirect supports many secure protocols and services including IPsec, which is a protocol that allows for strong authentication, confidentiality, and integrity of communications with industry-approved encryption methodologies on the network.

Figure 1. IPG Security Framework


3. **Effectively monitor and manage** – HP Web Jetadmin allows a fleet of products to be managed manually, and can automatically recognize and configure newly installed products that are deployed on enterprise networks. HP Web Jetadmin manages any product that supports the Simple Network Management Protocol (SNMP) printer Management Information Base. It uses SNMP v3.0 to facilitate authenticated and confidential management of networked products.
4. **Secure the document** – Many organizations print sensitive documents such as checks, prescriptions, certificates, and contracts. The fraudulent copying, alteration, or counterfeiting of these documents can cause significant financial loss and damage to an organization's reputation.

   HP and its partner TROY Group provide security fonts and anti-copy paper to help prevent fraudulent copying, as well as a security toner that releases red dye onto the page when alterations—be it mechanical or using solvents—are attempted. HP and TROY Group also provide security features designed to prevent counterfeit creation of documents.

HP works with organizations to assess their requirements and recommend an approach that meets the organization's unique business needs. HP offers modular security solutions to help optimize an organization's infrastructure, manage its environment, and improve its workflows. Or, HP can help build on an existing information technology environment by helping to establish a comprehensive plan that implements the best solution for today and builds a secure foundation for the future.

[1] ComputerWeekly.com, March 26, 2007
[2] **www.privacyrights.org/ar/ChronDataBreaches.htm**
[3] **www.hp.com/go/secureprinting**

The HP MFP Security Checklist is certified by the National Institute of Standards & Technology (NIST), and provides industry "best practices" for ensuring secure use of MFPs in an enterprise environment. This checklist applies to the entire portfolio of HP LaserJet MFP products.[3]

## What's new?

**The HP Access Control Printing Solutions (HPAC)** – A set of solutions designed to control and protect access to imaging and printing products, documents and information; mitigate compliance and security risks; and facilitate tracking, monitoring and managing of information about documents. This comprehensive set of printing solutions helps automate manual processing to streamline information workflows, deliver greater compliance readiness, reduce the risk of error, and increase operational effectiveness of current and new printing and imaging products.

This solution suite is ideal for delivering what HP calls the "four A's" of security—Authentication, Authorization, Audit and Accounting, and includes:

- HPAC Secure Printing – Prevents fraudulent printing use and facilitates compliance
- HPAC Secure Pull Printing – Enables on-demand retention and retrieval of encrypted print jobs with enabled products, providing confidentiality on shared products
- HPAC Job Accounting – Tracks, manages and accounts for all print, email, copy, and fax activity with HP products, and facilitates print cost recovery across the organization

**The HP High-Performance Secure Hard Disks Solution** – A simple, fast, and automated way to protect sensitive data. This cryptographic solution helps secure information on your HP printer or MFP while maintaining the product's throughput and performance. Advanced Encryption Standard reduces the risk of stolen data and increases employee, customer, and partner confidence in the safety of information within an organization.

## How do you get started?

### HP Security Advisor Workshop

Contact your local HP representative to set up an HP Security Advisor workshop and get a customized analysis of your imaging and printing environment. The workshop will help your organization assess its security vulnerabilities and begin building a strategy to eliminate security risks, reduce costs, and improve the efficiency of your organization's imaging and printing infrastructure.

### HP's ten steps towards security

It is essential that imaging and printing security becomes an integral part of your organization's overall security strategy! Take a proactive approach towards enterprise security with the following HP secure printing practices:

1. Know your business and understand what could make you an attractive target for "hackers" or other types of security attacks.
2. Perform a SWOT analysis on the security of your organization: what are the strengths, weaknesses, opportunities and threats related to your business?
3. Involve senior management and make sure that the security strategy is driven from the top down—management commitment is essential.
4. Make sure that the security strategy covers not only the technical aspects of how your organization carries out business, but is based on the operational, commercial and legal aspects of security.
5. Turn security from a cost center into a profit center—security is a business enabler, and provides flexibility and productivity features via secure printing environments (e.g., HP Pull Printing, HP MFP secure functions, etc.).
6. Start by writing a user-acceptable usage policy (AUP) to govern the use of e-mail, web, phone, instant messaging and other products—including printers.
7. Make sure that line managers enforce security policies across the organizations—IT must enforce firewall and content filtering policies, operations must work on disaster recovery and business continuity plans, HR must perform background checks (within the applicable regulatory framework) and work with IT to monitor AUP effectiveness.
8. Auditing is key—security is a proactive process, not a point solution.
9. Conduct security audits on your printing environment to align it with your current and future business requirements. If you are not currently using secure printing features, consider integrating this capability into your environment.
10. Make secure printing a way to increase overall corporate security and turn printing into an asset that enhances security, productivity, and ROI within the overall corporate environment.

To learn more, visit **www.hp.com/go/ws/printsecurityandcompliance.**



4AA2-3272ENW, November 2008