ASSESS, DEFINE *and* DEPLOY *your* IMAGING *and* PRINTING security solution

HP Secure Imaging and Printing Solutions

Does your imaging and printing environment put sensitive data at risk?

The amount of data we create is rising. With increased data come increased security risks and requirements. Organizations already use multiple authentication methods, including proximity badges, smartcards and PIN numbers to access buildings and to protect data on PCs and servers.

But is your imaging and printing environment protected? Did you know it needed to be? It does. At a time when sensitive data is ever more prevalent, organizations are failing to implement proper imaging and printing security measures. And at a cost.

Recently a financial institution reported an unauthorized employee was able to examine sensitive IPO information sitting in the output tray at the printer near his desk—and publicly shared it. That resulted in an estimated $7 million loss. In a study conducted by Ponemon, the median annual cost of cyber-crime for an organization is $3.8 million—with highest costs coming from information loss and business disruption.[1]

With the threat of lost revenue, fines, litigation and tarnished brand image resulting from security problems, it's not surprising that 50 percent of enterprises indicate their security budgets are rising.[2]

So how do you assess whether your imaging and printing environment is properly protected? How do you secure an entire fleet of hundreds or even thousands of printers, MFPs and scanners enterprise-wide? How do you control countless users, accessing countless machines for countless reasons? HP Imaging and Printing Security Solutions can help.
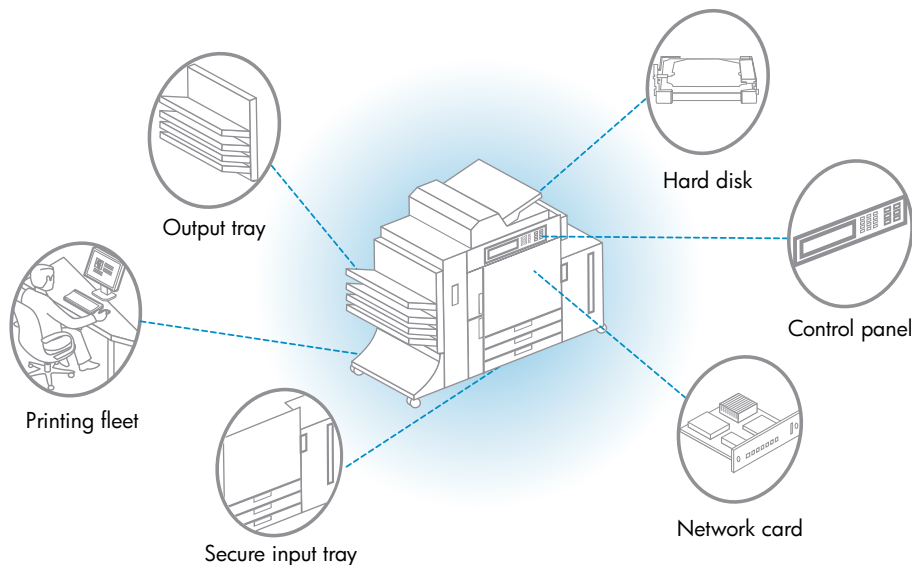

Figure 1. Imaging and printing vulnerability points

Six imaging and printing vulnerability points

There are a variety of security gaps that imaging and printing devices can introduce. Once you understand them, they are easy to address.

1. **Output tray:** This is the most common vulnerability point. How many documents are sitting on output trays all around your business right now? Are they confidential? Who can see them, pick them up and share them?

2. **Hard disk:** Did you know printers and MFPs are capable of storing files sent to the printer on a hard disk? When a printer leaves your business, is sent out for repair or returned at the end of a lease, it could leave with a drive full of sensitive information.

3. **Network:** It's surprisingly easy to intercept print jobs as they travel over the network to a printer or MFP. An Internet search for "sniffers" will pull up numerous applications to accomplish this.

4. **Control panel:** MFPs are powerful devices that can print, copy, scan, fax and e-mail. If you don't have visibility and control over access and use of the device, you can't control use and prevent abuse.

5. **Input tray:** Many organizations use special media to print checks, prescriptions and official documents. Without secure input trays, that media can be tampered with or stolen.

6. **Fleet control:** Actively assessing, managing and auditing print security across an entire printing environment takes consideration and know-how. Controlling a handful of printers is easy enough, but systematically securing an entire fleet of devices requires thoughtful planning and a tailored solution.

Many of these vulnerability points seem quite obvious once you consider them. Some of them may have already addressed. Others may never have crossed your mind. By assessing your fleet and determining what types of devices you have, how they are used and by whom, you can implement security features and solutions that greatly reduce the chance of a breach.

Close your imaging and printing security gaps.

Now that you're aware of the vulnerability points, how do you go about addressing them? What solutions can your organization put in place to close those imaging and printing security gaps? Below are solutions for the six vulnerability points we just covered:

1. Employee authentication and pull printing

Keep hard copies from falling into the wrong hands with employee authentication. Authentication technology includes PIN printing, proximity badges, smart cards and biometrics such as fingerprint scanning. These technologies verify the employee and only print hard copies when the employee is at the printer to pick up the document.

Pull printing can also help. This technology keeps documents on a secure server. The document is then "pulled" when the employee is authenticated at any printer connected to the server using one of the verification methods above.

2. Securing printer and MFP hard disks

HP LaserJet solutions offer HP High-Performance Secure Hard Disks that encrypt all the data received by and stored on the printer. HP Secure File Erase and HP Secure Disk Erase allow you to systematically erase data file by file or wipe all data on a hard disk.

3. Protecting data sent over the network

Be sure to encrypt all print jobs sent over the network. Encryption solutions such as IPsec/IPv6 (embedded on most current HP devices and also in the external HP Jetdirect 635n or 690n cards for older devices), HP Access Control Secure Driver Plug-in and solutions from third-party sources can make your files nearly impossible to read if rerouted or intercepted.

4. Controlling printer access and feature use

If you verify printer users, you can control who uses which printers. But you can also control who has access to IT and administrative printer settings and who has access to faxing, color printing or other features. HP Web Jetadmin Software, a powerful monitoring and management tool for your printing fleet and HP Access Control can help you establish control and secure printer usage.

5. Preventing paper and media tampering

Many organizations use specialized paper and media for printing sensitive material. HP offers secure paper trays that prevent unauthorized access to specialty paper. HP also works with partners that provide secure micro toner and even magnetic ink character recognition technology that stains when tampered with. These technologies help prevent tampering and altering of your sensitive documents. And there are HP solutions that print codes to track and audit individual documents.

6. Managing and monitoring your entire fleet

You can't control what you don't know. Deploy a complete imaging and printing management and monitoring solution such as HP Web Jetadmin. It allows you to track usage, audit practices, set defaults and control access from the highest level all the way down to the smallest feature. HP can show you how to do it yourself, or we can provide it as a service.

Plan and deploy your imaging and printing security solution.

Security saves money.

Security as part of a managed imaging and printing solution saves money. For instance, companies implementing PIN and pull printing can realize up to a 30 percent reduction in printing costs.

Depending on the scope and size of your imaging and printing security needs, you can plan and execute a solution in a variety of ways.

- HP provides a self-assessment checklist and tool, the HP Security Action Plan, that you can use to scope your fleet and determine your security requirements. You can then implement any built-in security features and/or procure and deploy specialty imaging and printing solutions on your own.

- HP also offers a comprehensive workshop that can include assessments for nearly every facet of your printing environment. We'll sit down with you to identify fleet-wide vulnerability solutions that increase security and may decrease costs.

- You can use HP Managed Print Services to develop a custom solution that takes care of the imaging and printing security areas you don't want to manage yourself. Or HP can take on everything and deliver a full-service, no-hassle solution.

How do you get started?

- Learn more about HP imaging and printing security solutions at **www.hp.com/go/secureprinting**.
- Check out the HP imaging and printing Security Action Plan at **www.hp.com/go/SecurityActionPlan**.
- Or to schedule an imaging and printing security assessment and workshop contact your HP sales representative or Executive.Programs@hp.com.

1. First Annual Cost of Cyber Crime Study, Benchmark Study of U.S. Companies. Sponsored by ArcSight and independently conducted by Ponemon Institute LLC, July 2010.
2. Ernst & Young. "Outpacing Change: Ernst & Young's 12th Annual Global Information Security Survey." November 10, 2009 http://www.ey.com/Publication/vwLUAssets/12th_Annual_Global_Information_Security_Survey/$FILE/12th_annual_GISS.pdf.

HP three-part approach

HP works with you to assess, deploy and manage an imaging and printing environment tailored to meet your business needs, while helping you reduce costs, conserve resources and simplify document-intensive processes.

Optimize infrastructure	Manage environment	Improve workflow
HP can help you achieve a balance between your total cost of printing and your needs for user convenience and productivity.	Working together, HP can help you maintain your optimized infrastructure while improving business efficiency and tightening security.	By streamlining your document-intensive processes, HP can help you deliver a more efficient environment for capturing, managing and sharing information.

You can discover more about all of these options by visiting www.hp.com/go/secureprinting.

HIT **PRINT**
INTELLIGENTLY