



Hardcopy Security: *An Open Door*



Don Wright
Director, Alliances & Standards
Lexmark International
don@lexmark.com

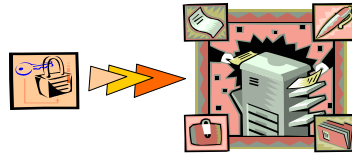
10/29/2003

LEXMARK

1

Agenda

- Thoughts on Security
- What is Hardcopy Security?
- Components of Hardcopy Security
- Who needs Hardcopy Security and Why?
- The existing Hardcopy Security Landscape
- What is needed and how do we get there
- Questions



10/29/2003

LEXMARK

2

What, me worry?

- “Commitment to Security & Privacy is the problem not the lack of technology. Do you really need to ask ‘What’s the business case for adding security to your products?’ ”
 - ❖ Nicholas Donofrio, Senior Vice President, Technology and Manufacturing, IBM
- “Valuable information must be protected no matter what form it takes or where it is located. An organization’s customer list has the same value whether in hardcopy form or an electronic file...”
 - ❖ Kevin Mitnick, “The Art of Deception”
- “Spam, security breaches, denial of service have become ‘Weapons of Mass Disruption.’ ”
 - ❖ Bill Gates, Chairman and Chief Software Architect, Microsoft
- “Information never stays in computers; it moves onto paper all the time. Information is information and, for an attacker, information in paper files is just as good as information in computer files.”
 - ❖ Bruce Schneier, “Secrets & Lies”

10/29/2003

LEXMARK

3

What is “Hardcopy Security” ??



For the purposes of this discussion, “Hardcopy Security” is



The measures, methods and procedures taken to guard against an attack on, theft of, espionage against, or the sabotage of, the devices, components or systems used to print, scan, copy, transmit, receive or store documents on (or intended to be on) paper or other human readable media.



10/29/2003

LEXMARK

4

Components of Hardcopy Security

■ Physical

- ❖ Theft prevention (Memory Cards, Hard disk drives, etc.)
- ❖ Disposal of integrated flash memory and/or hard disk drives

■ Authentication

- ❖ Who are you and how do you prove it? Userids? Passwords? SmartCards? Biometrics?
- ❖ Federated Identity Systems such as Liberty Alliance or Passport

■ Authorization

- ❖ Are you authorized to print? Copy? Scan?
- ❖ Is that your print job being held for you in the printer?
- ❖ How are authorization levels maintained, managed, transmitted?

■ Privacy

- ❖ Protection/Encryption of data transmitted to or from device
- ❖ Protection/Encryption of data residing on device
- ❖ HIPAA, Gramm-Leach-Bliley Act (Protection of Nonpublic Personal Information)
- ❖ Protection of the physical output, i.e. the paper

10/29/2003

LEXMARK

5

Components of Hardcopy Security

■ Monitoring / Auditing

- ❖ Should you track who scanned or copied what?
- ❖ Knowledge of printing/scanning usage, timing, volumes can be insightful.
- ❖ Who is attempting unauthorized activities?

■ Device Management

- ❖ Unauthorized configuration changes (disabling safeguards)
- ❖ Unauthorized "firmware" updates (re-enabling or bypassing disabled functions)

■ Document Security

- ❖ Confidentiality, Integrity, Authenticity
- ❖ Non-repudiation, Authentication, Access Control

■ Customer perceptions (correct or incorrect)

- ❖ Use of fax modem connection to break into corporate networks
- ❖ Use of device as source of denial of service, e-mail relays (spam), etc.

10/29/2003

LEXMARK

6

Why Worry about Hardcopy Security?

■ Isn't it just good business practice?



Do you want your competitors, either internal or external, "sniffing" your PowerPoint charts on the way to the printer?



Do you want your confidential personnel output sitting in the output hopper of your printer while you're stuck in a sudden 2 hour emergency meeting?



Do you want your scanned financial statements sitting on a server as an easily readable .pdf file when the next security breach is found that gives "root" access to everyone?

10/29/2003

LEXMARK

7

Hardcopy Security and the Law

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) requires health care organizations to protect the privacy and security of confidential health information and calls for standard formats for electronic transactions. These standardized national requirements apply to the electronic transmission of patient history and health records such as health insurance enrollment detail and claims. The need to maintain confidentiality and privacy of medical information and rules for medical document security, including standards related to data integrity and encryption, are also outlined in HIPAA.

GLB

The Gramm-Leach-Bliley Act (GLB) contains a Safeguards Rule which requires financial institutions to have in place a comprehensive security program to ensure the security and confidentiality of customer information. This includes the identification of employee coordinators, the identification of foreseeable internal and external risks, the implementation of safeguards to address the risks, and the regular adjustment of the programs in light of developments that may materially affect the program.

10/29/2003

LEXMARK

8

Who ^{doesn't} need Hardcopy Security?

People on a deserted island without internet access and with their printers connected to their PCs with a parallel cable.



Your kids printing out their art projects at home.



Anyone else?



10/29/2003

LEXMARK

9

Existing Standards for Hardcopy Security

- No comprehensive standards specific to hardcopy security currently exist.
- Components of some existing standards could be applied to the hardcopy environment, for example:
 - ❖ Common Criteria's "Residual information protection (FDP_RIP)" for the contents of an integrated hard disk.
 - ❖ Common Criteria's "Cryptographic operation (FCS_COP)" for sending an encrypted print job.
 - ❖ Many others
- Some information security policies deal lightly with hardcopy security but then only from the perspective of information classification.
- However, while these basic functions may be useful, they do not address the aggregation of functions for a printer such as what is contained in ISO/IEC 17799 "Information technology – Code of practice for information security management" for computers and workstations in general.

No standards → No Checklists!

10/29/2003

LEXMARK

10

What is needed?

- Standards for hardcopy security covering all aspects of printers and other multifunction hardcopy devices and their usage, including:
 - ❖ Applications
 - ❖ Operating system
 - ❖ Transmission of the print job or scan job
 - ❖ Copying
 - ❖ Job hold for user
 - ❖ Physical Security
 - ❖ Device management
 - ❖ User authentication
 - ❖ Etc.
- Checklists, guidelines and best practices documents to assist IT organizations in planning and implementing a hardcopy security plan.
- Assessment and Certification standards to measure compliance with the above standards.

10/29/2003

LEXMARK[™]

11

How do we get there?

- Lexmark is taking the initiative now to put together an effort to develop the necessary standards to address hardcopy security.
- A number of the leaders from the hardcopy industry are here today to kick-off this effort.
- We will include not only these and other hardcopy manufacturers but also the appropriate users from the commercial and government sectors.
- From these standards, appropriate checklists and other tools to assess, measure and certify compliance can be developed.
- We are considering several venues for this work including the IEEE Computer Society's Information Assurance Standards Committee.

10/29/2003

LEXMARK[™]

12

Questions?

Thanks for your attention!!