EDPACS
THE EDP AUDIT, CONTROL, AND SECURITY NEWSLETTER

JANUARY 2010 VOL. 41, NO. 1

DIGITAL MULTIFUNCTIONAL DEVICES: FORENSIC VALUE AND CORPORATE EXPOSURE[1]

AL MARCELLA, Ph.D., CISA

Abstract. Traditional forensics professionals use, among other tools, fingerprinting blood splatter and ballistic analysis, DNA typing, and forensic pathology to make their case. Infosec professionals have to develop new tools for collecting, preserving, examining and evaluating electronic evidence in an effort to establish intent, culpability, motive, means, methods and loss, resulting from cyber-based crimes. Considering the increasing complexity of technology, and, as a result, the devices that may contain latent and incriminating digital evidence, due to a migration from aged analog devices to state-of-the-art digital multifunctional devices (MFDs), this article discusses these MFDs and their importance/role in cyber forensic investigations and the exposure, that they may represent to un- and under- prepared organizations.

INTRODUCTION

The need to remain vendor neutral and to avoid the appearance of favoring any specific product, service, or vendor is paramount when one undertakes a research and writing project. To every rule there is usually an exception, and as fate would have it, such is the case in the preparation of the material you are about to read in this article.

Considering the increasing complexity of technology and as a result, the devices which may contain latent digital evidence, due to a migration from aged analog devices to state-of-the-art digital multifunctional devices (MFDs), the discussion of these MFDs and their importance/role in cyber forensic investigations and the exposure which they may represent to un- and under-prepared organizations necessitated the research and writing of this article.

[1] This article is based on material originally published in *Cyber Forensics* II: A Field Manual for Collecting, Examining Evidence of Cyber Crimes, 2nd Edition, 2007, © Taylor & Francis, and is reprinted with permission.

ASSESSMENT OF PRODUCTS

The initial investigation centered on examining the potential which photocopiers may have as a source for latent data and the potential necessity for the cyber forensic investigator to include these devices in the scope of his/her investigation. Additionally, examined by default, was the potential exposure to the confidentiality of data, which would befall organizations where data leakage to occur via an MFD.

It would make little sense to base an investigation of potential latent data, residing on a photocopier, if it could be proven that the machine itself lacked basic security features that might render any potential evidence, which may have been collected from the machine, inadmissible or at least highly suspect with regards to its integrity. Checking with the National Vulnerability Database (NVD) (http://nvd.nist.gov) prior to beginning a forensic examination of a MFD may provide additional useful information for the auditor/investigator.

The NVD is the only database that is completely based upon the Common Vulnerabilities and Exposures standard vulnerability dictionary. It is the only database providing Common Vulnerability Scoring System (CVSS) scores for all Common Vulnerabilities and Exposures (CVE) vulnerabilities. And it is the only vulnerability database that integrates Open Vulnerability Assessment Language (OVAL) queries.

The most important usage of the statistics engine is to look at the past history of a product as an indicator to see whether or not it is likely to be vulnerable in the future. For example, the statistics engine has revealed that some major software vendors have exponentially increasing numbers of vulnerabilities being discovered in their products every year while the vulnerability discovery rate for other software vendors is staying steady or falling.

Early in 2003, Sharp Electronics commissioned a survey of 1,100 IT professionals to gauge their level of awareness about the security holes posed by common office equipment such as copiers, printers, faxes, and scanners. The results were startling. The survey revealed that information technology professionals are largely unaware or uncertain of the potential risk of the theft of documents from office equipment.

If you have information of interest to *EDPACS*, contact Dan Swanson (dswanson_2008@yahoo.ca). *EDPACS* (Print ISSN 0736-6981/Online ISSN 1936-1009) is published monthly by Taylor & Francis Group, LLC., 325 Chestnut Street, Suite 800, Philadelphia, PA 19106. Periodicals postage is paid at Philadelphia, PA and additional mailing offices. Subscription rates: US$ 311/£187/€248. Printed in USA. POSTMASTER: Send address change to *EDPACS*, Taylor & Francis Group, LLC., 325 Chestnut Street, Suite 800, Philadelphia, PA 19106.

The survey revealed:

- 47 percent of respondents erroneously believed that their copier/printer did not contain a hard drive.
- An additional 30 percent said they simply did not know whether the device contained a hard drive.
- 65 percent said copier/printers presented little or no risk to data security.
- 5 percent of survey respondents were aware of any data security breach in copier/printers.

The results of the study underscore the convergence of several trends: the increased use of sophisticated, high-performance digital technology in office equipment and the shift toward management of the increasingly connected devices by IT personnel who focus more on their computers than on peripheral devices (Cybuck, 2003).

DATA SECURITY AND LATENT ELECTRONIC EVIDENCE

After a review of the information provided in the NVD, it is also very apparent that MFDs pose a significant, here-to-date, almost overlooked and underestimated security exposure for any organization in which MFDs are present.

The investigation into the exposures created via MFDs led to an examination of what methods organizations use to secure the varied MFDs operating within their many offices. Surprisingly, the investigation found little awareness of the potential security exposure or legal liability, which faces an unprepared corporation. There was also little evidence found in the way of hard-, soft- or firm-ware designed to protect data at rest.

In an effort to explore further and to bring to the reader's attention the connection and critical importance which MFDs have to a cyber forensic investigation, the author contacted Peter Cybuck, Associate Director Solution and Security Business Development at Sharp Electronics Corporation. Peter is acutely familiar with and deeply committed to securing content on MFDs. Peter is a member of The Software Assurance (SwA) Acquisition Working Group, NSA's High Tech crimes group, among other professional organizations.

In discussions and interviews with the author, Peter has provided his insights, expertise, and comments regarding the varied vulnerabilities associated with MFDs. Peter noted for example, "that Flash memory usually used in connection with fax applications can retain data as long as a hard drive. Your IPOD Nano doesn't lose your songs when you unplug it, thus, your copier also won't lose the documents in Flash Memory either. Copiers with RAM can be on a network plugged in for weeks holding document data in RAM, so clearing RAM is also an important security consideration."

When a document is printed, copied, scanned, or faxed, the temporary data stored/buffered in memory is overwritten (as with Sharp's DSK product) up to seven times, rendering it unrecoverable (Sharp Electronics, 2006).

"The Sharp DSK product overwrites encrypted data. The reason is that there is always the possibility that a power failure or even a

machine mechanical failure (jam) might prevent the overwrites from executing. By storing the confidential data as encrypted data it is protected even if the overwrites never execute (at the end of a "job").

"Seven separate overwrites are used by Sharp to assure a statistically significant degradation of magnetic remnant data. One or two . . . even three overwrites used by some software can leave evidence on the magnetic surface of the drive sectors that very sophisticated labs might recover. In the case of the Sharp MFDs, the lab, after seven overwrites is very unlikely to recover anything beyond molecular noise and any fragments discovered would be fragments of a strongly encrypted file" (Cybuck, 2007).

This point is both important to the auditor and cyber forensics investigator in that if a MFD is so well protected, that the potential of identifying and obtaining latent data is remote, knowing this will help to initially limit the scope of the audit/investigation as well as help determine the feasibility of pursuing this line of investigation to begin with.

ISSUES AND CONCERNS

The risk of data theft or misuse in today's competitive marketplace is real—whether due to a malicious network attack, disgruntled employee, or electronic eavesdropping. Increasing this risk, as usually seen, is the threat from inside. The service agents that can swap drives and memory modules as they perform routine maintenance of corporate MFDs are a prime source of exposure. When was the last time you stood and watched as the service repair person performed their job? Are you positive that he/she did not remove a hard drive full of potentially confidential data? You did stand there and watch while the service/repair work was performed, didn't you?

The resellers of MFDs removed from facilities when leases expire are also a major threat. They often mine used, decommissioned machines for confidential data.

1. Does your photocopy lease agreement call for and guarantee the removal of the hard drive, prior to the machine being "turned"?
2. Who receives this drive?
3. What policies are in effect to wipe the drive (and certify that it no longer contains data) prior to its disposal?
4. Should you wipe the drive?
5. What if six months from now you need those data on the drive as evidence, how will you retrieve them, and from whom?

Every day, billions of pages of confidential information—medical records, legal documents, and financial data—are produced and distributed using sophisticated digital office systems—printers, copiers, facsimile, and MFDs. Many businesses may be unaware that whenever these devices are connected to a network, the risk of unauthorized access and data loss exists. Even as a stand- alone device, these "intelligent" systems retain latent document images, potentially exposing sensitive information.

When questioned about additional security exposures both the cyber forensic investigator as well as the internal controls professional should consider, Peter responded "the often anonymous

communication capabilities of today's MFD's deserves some attention. They can often be used to email documents out of a facility without being logged to a sent mail folder. Documents (print as well as scan files) sent to or from the MFD over a network unencrypted can be sniffed by off the shelf software and captured by attackers. Sharp provides the option of sending encrypted PDFs and encrypted print files over the network to and from the MFD. The Sharp MFD firmware is capable of both encryption and decryption."

This means that mission-critical data and documents are vulnerable to serious security breaches, yet organizations often focus attention and resources on securing their network, PCs, and servers, not device input/output equipment. This leaves the back door open to anyone intent on undermining your business interests—attackers, employees, service agents, and competitors alike.

Failure to take steps to protect information assets has serious consequences, perhaps exposing an organization to liability claims, financial loss, and criminal penalties (Sharp Electronics, 2006).

As part of a thorough investigation, the auditor and the cyber forensic investigator must consider any device capable of storing data as a potential source of electronic evidence, important to his/her audit/investigation.

The technical growth and embellishment of the MFD has resulted in an internal re-configuration of the machine now (and for some time) to be outfitted with a hard drive. Yes, a hard drive, the same type and almost the same capacity, as the hard drive which sits inside your PC workstation on top of or beneath your desk, as well as Flash Memory in both high and low end units without drives.

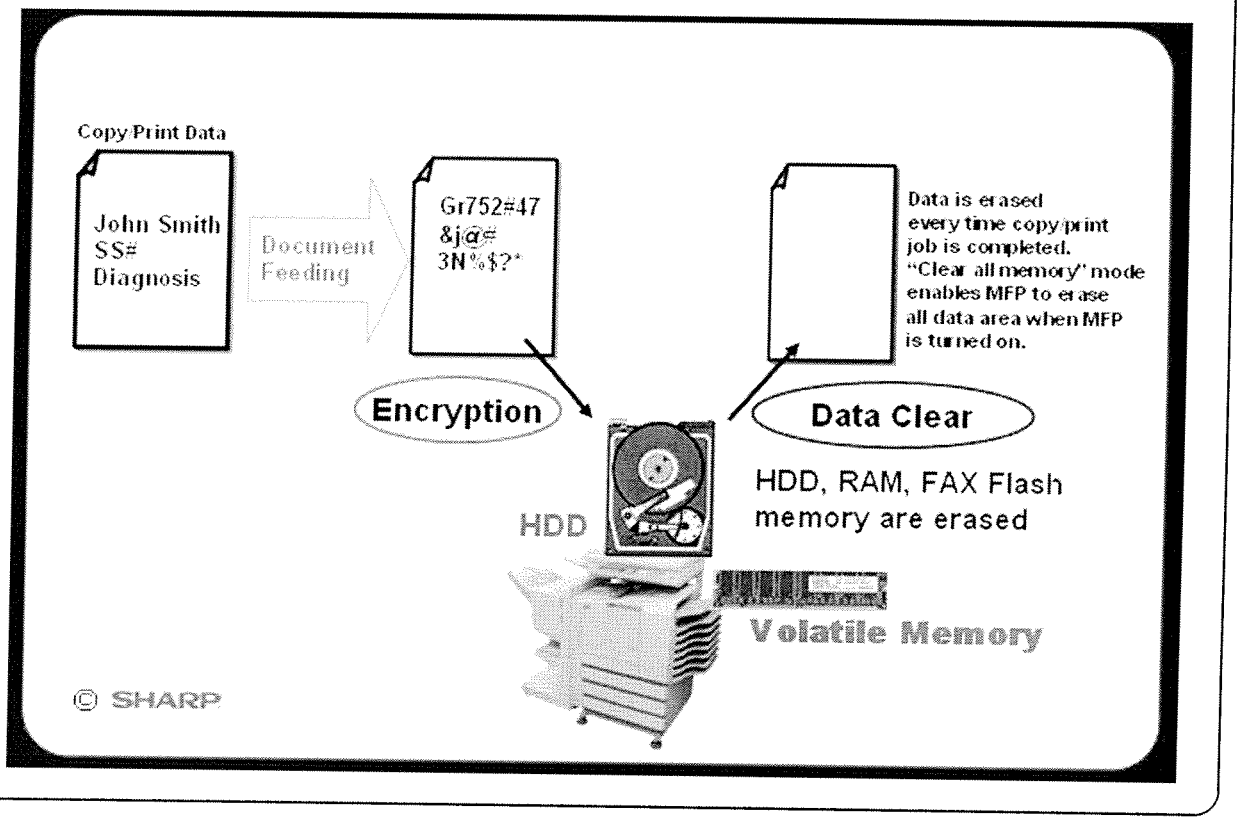
Stop and think for a moment, what are all of the access, security, and integrity concerns/issues you had (have) with controlling unauthorized access to data residing on your (or your end user's) PC or laptop—you now have (or should have) the same concerns/issues with the data which resides on your organization's photocopier's hard drive. In fact, you should probably be more concerned, be more worried, be more afraid—the hard drive on your photocopier and the data residing on it, is completely exposed, unprotected, and accessible to anyone with the right tools and know how (which by the way IS NOT rocket science). (Figure 1).

THE TECHNICAL STUFF

A rough estimate of the storage capabilities of a photocopier's hard drive indicates that at any one time, approximately 125,000 to a quarter million pages of text (of images of jobs, copied, scanned, e-mailed, etc.) can remain/reside, on the hard drive of a corporate photocopier. Those data, those stored images represent a significant amount of potential electronic evidence, which may prove valuable in a cyber forensic investigation, and equally represent potentially confidential information on internal organizational activities or an individual's personal information (think identity theft, The Health Insurance Portability Rights and Accountability Act [HIPAA] of 1996, The Family Educational and Privacy Act of 1974 [FERPA or the Buckley Amendment] violation!).

Most copiers do not sequentially store the documents copied. If they did they would quickly run out of memory. Many overwrite

Figure 1 *Encryption and data Clearing of photocopied material.*



a temporary buffer memory used to capture the copied pages. Other MFDs, however, utilize the memory capability differently, such as a print spooler in the MFD or so-called "secure print mailboxes" used to store print jobs until the user walks up to the unit, enters a PIN or password, and retrieves the documents while at the copier can not only indefinitely retain more page data but retain it in a format (as PCL or Postscript files) that are easy for even amateurs to recover (Cybuck, 2007).

Not only do these data represent "pools" of potentially latent electronic evidence, they also represent a potential legal and financial exposure to the corporation—a significant internal security exposure/risk/vulnerability. (Figure 2).

Left unprotected, however, MFD devices can create a breach in your security architecture and unauthorized parties can gain access to intellectual property and confidential information (Sharp Electronics, 2005).

Most MFDs in operation today, in almost every major organization around the globe, include a great deal of memory, even hard drives similar to those in desktop computers. The memory is used to buffer the documents that are copied, printed, scanned, and faxed. What most users do not realize is that the document information remains in the memory when they walk away from the machine.

Figure 2 *Vulnerability points resident in an MFD.*

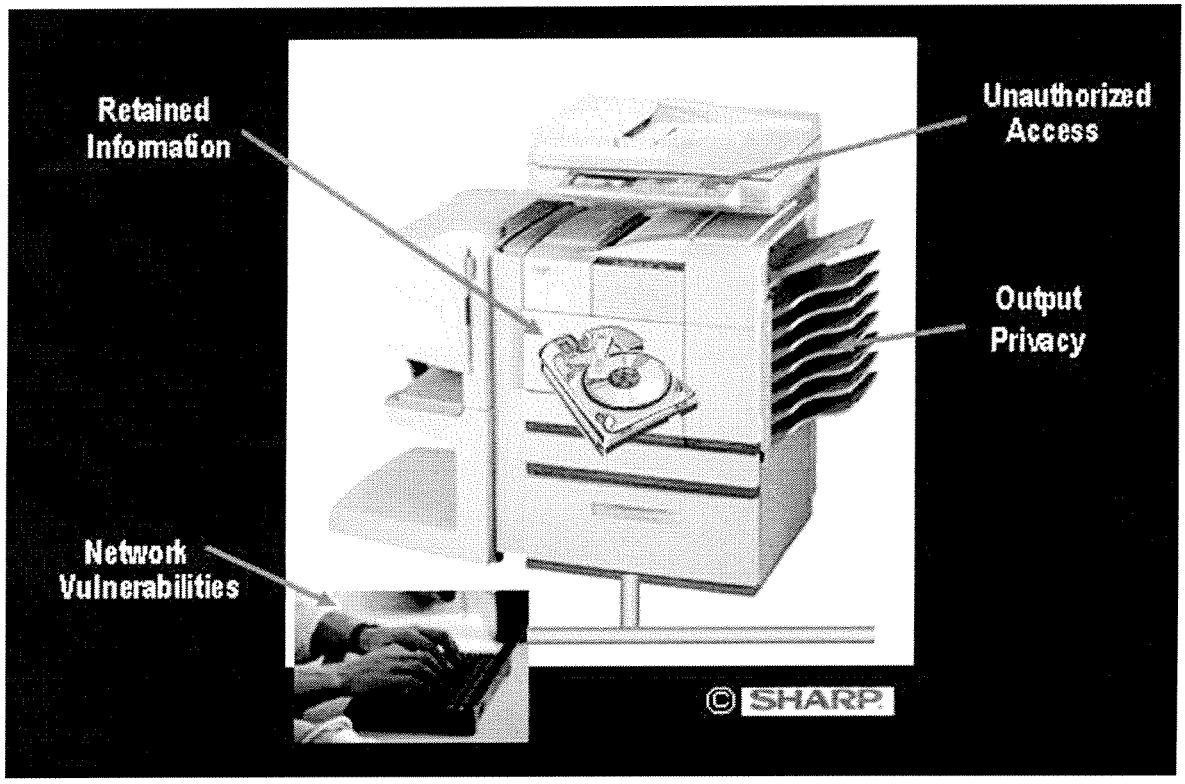
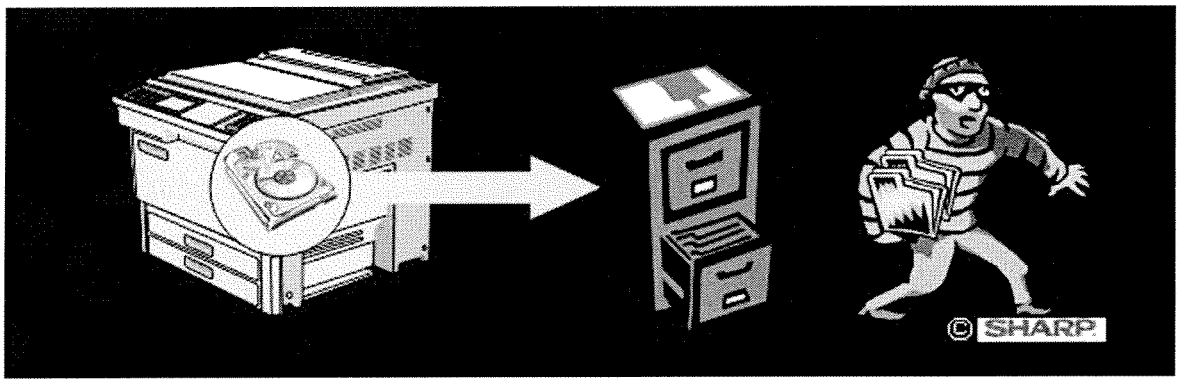
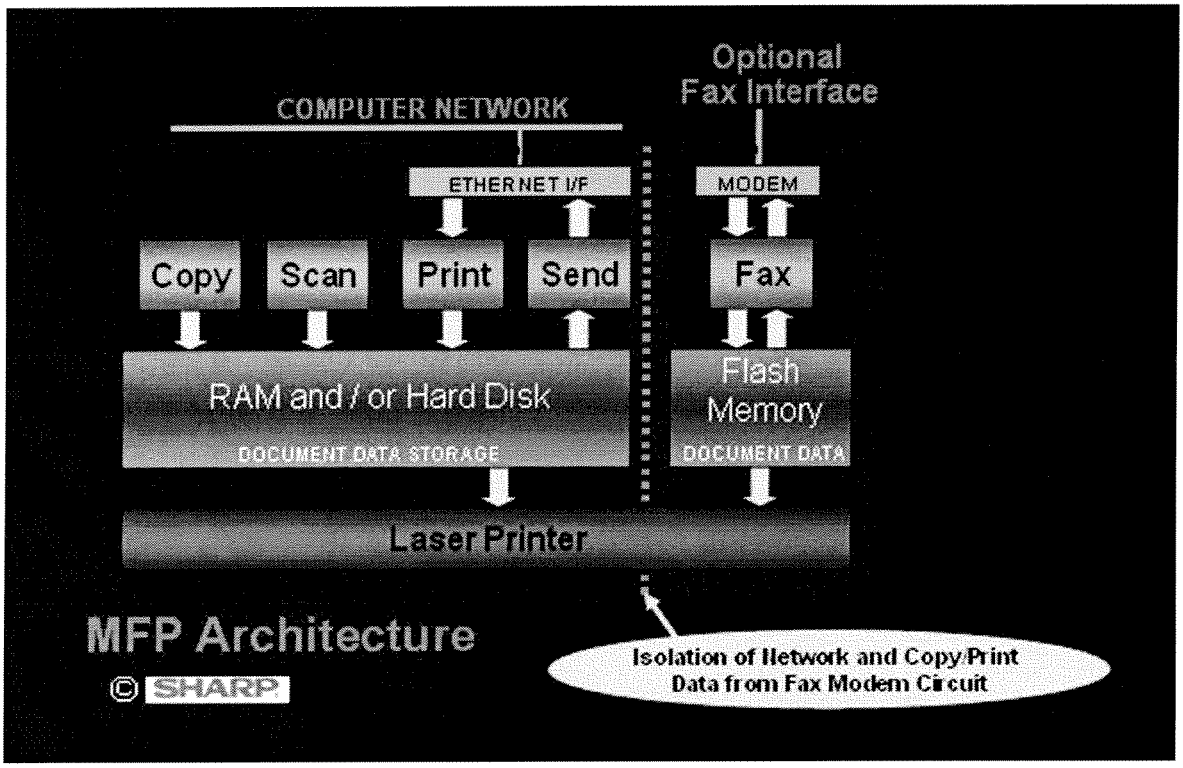


Figure 3 *Privacy and compliance risks inherent within MFDs.*



Attackers are starting to see these devices and document processing devices as the weakest link in many networks and they are starting to draw unwanted attention. There is a high potential to retrieve and intercept confidential document data and they can be used to launch attacks on user networks (Cybuck, 2005) (Figure 3).

Figure 4 *Isolation of network and copy/print data from fax/modem circuits.*



THE FORENSIC APPLICATION

Most incidents involve employees and their access to devices that process sensitive information—including the copiers, printers, scanners, and fax machines they use every day (Sharp, 2005).

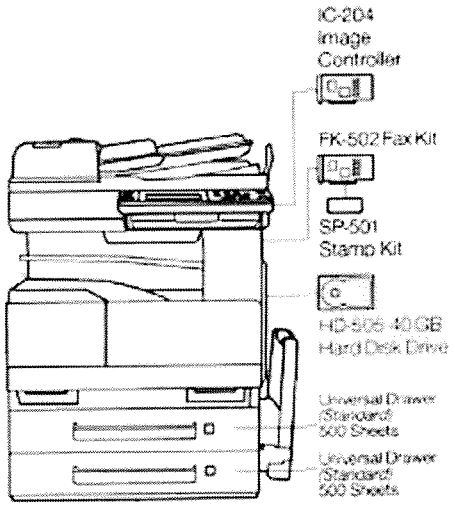
There are a multitude of factors which must be considered before the auditor/investigator should begin an examination of a MFD. The first consideration is to determine the level of security (or lack thereof) which may be protecting access to and control over the MFD. If robust security (such as Sharp's DSK, for example) is in place, and this is verifiable, the likelihood of uncovering any useable electronic evidence is highly unlikely, and the auditor/investigator could eliminate these MFDs as potential sources for review and examination.

If, on the other hand, there appears to be little or no security over the MFDs, then the auditor/investigator should proceed and consider the possibility that specific MFDs may require a forensic examination. (Figure 4).

THE EXAMINATION PROCESS

Presented with the question, "How exactly would an auditor or a cyber forensic investigator access stored images retained on the

Figure 5 *MFD's hard drive location.*



hard drive of a MFD and similarly, how would someone with less honorable or legal intentions acquire these data?" Peter Cybuck provided the following response:

Drives used in MFDs use PC-like interfaces and can easily be mounted using standard cables on PC's. If the MFD uses a Windows or Unix operating system it can be very easy to locate stored files. If proprietary disk control software is used (as is the case with the Sharp MFDs) the data may only appear as binary fields on undocumented drive sectors.

The binary document data might also represent document images compressed using proprietary undocumented compression technology. Note that the copied documents are not stored as ASCII files. They are images, so if a small part of a document is recovered it might just be white space, as in the margin of a letter. If a small part of a word or text document is recovered it might provide a significant amount of information. Much more "data" must be recovered from a copier drive and much more analysis is necessary before it is understood.

That does not mean that it is not there and not recoverable. It does mean that depending on the architecture of the MFD and its operating system it might or might not be vulnerable to low level attackers. The use of off the shelf vulnerable mass market operating systems can make an MFD much more vulnerable. (Figure 5).

A STEP BY STEP LOOK AT EXAMINING A MFD'S HARD DRIVE

1. Mount the drive using a compatible computer cable.
2. If a computer disk operating system was not used search the Internet for software that permits you to examine drive sectors.
3. At a minimum you will see binary arrays on the sectors that represent data.
4. Decoding it is possible but can be non-trivial if the data is not in the form of traditional computer files such as PCL or Postscript print files or coded PDF files using ASCII characters.

5. Note that log files and audit files may be more easily decoded since they will very likely be stored as ASCII files not compressed binary files.
6. If individual user access profiles were used to control MFD access this can provide useful information if not document data.

THERE ARE NO ABSOLUTES

After conducting such an audit (or for legal reasons an examination), in the collecting and documenting of electronic evidence, there is no guarantee that said evidence will be useable, lead to a conviction, or justify the time and energy expended, nor the expense, for what evidence may have been obtained.

If the organization did not restrict access to or use of the MFD by even the simplest of measures, requiring a personal access code to operate the MFD for example, to scan and transmit the schematics, then literally anyone could have had the opportunity to access and use the MFD.

Implementation of specific security features at the initial point of contact with the MFD may help to better establish the necessary security, date, time stamp, and audit trail required to ascertain with a greater degree of certainty, who is responsible for utilizing the MFD in question, and who leaked confidential, proprietary information to external third parties.

While there are many other MFD vulnerabilities most don't leave a data trail that can be mined for evidence. Most MFDs today can send documents to local computers as well as to e-mail servers and are often setup with customized "soft" buttons on the display that make it very easy to send to local desktops or network drives.

Simply looking at the list of scan destinations on the local copier might provide clues as to which computer was used to collect the scanned documents. It can also point toward possible network drives that might have been used to store even temporarily the scanned documents. It should be much easier to recover the documents from the desktop or network drives, the mail server address programmed into the MFD points toward another computer with a drive that could be mined for the document files. (Cybuck, 2007)

SUMMARY

Today's MFDs pose a considerable risk in the unsecured data which may be accessible to unauthorized individuals, violating such legislation as FERPA, HIPAA, The Sarbanes-Oxley Act of 2002 (SOX), The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, SOX, GLB, and so on and exposing the organization to legal and financial sanctions. Some of these laws forbid the transmission of confidential files like health records across state or provincial borders through the public Internet unless they are encrypted. Additionally, MFDs add another source of potential electronic exposure, which should be considered as a source of potential evidence by the cyber forensic investigator and as a potential internal control exposure by the auditor as each establishes the scope of his/her audit/investigation.

The author personally thanks Peter Cybuck for giving his valuable time to discuss security issues related to uncontrolled MFDs and to provide his insights and expertise on the subject of MFDs and their role in a cyber forensic investigation.

This article is taken from Dr. Marcella's recent book *Cyber Forensics II: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, and reprinted with permission of the publisher Taylor & Francis Group, ISBN 0-84938-328-5.

This article should be cited as such: Marcella, A., Menendez, D. (2007) Cyber Forensics II: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Second Edition, New York: Taylor & Francis Group, ISBN 0-84938-328-5.

References

Cybuck, P. (March 2003). Machine talk: What secrets are your office equipment passing along? Security Products, p. 34. Retrieved March 2007 from www.allcopyproducts.com/files/ItemFileA174.pdf

Cybuck, P. (May 2005). Accountable for security. Feature interview, Sharp Electronics Corporation, Sharp Plaza, Mahwah, NJ 07430-1163. www.sharpusa.com, www.ipac.ca, documents provided to author.

Cybuck, P. (2007). Associate Director Solution and Security Business Development at Sharp Electronics Corporation, personal interview February 2007.

Sharp Electronics Corporation (May 2005). Accountable for security. Sharp Electronics of Canada, Ltd., www.ipac.ca, Sharp Electronics Corporation Sharp Plaza, Mahwah, NJ 07430-1163. www.sharpusa.com, documents provided to author.

Sharp Electronics Corporation (December 2006). Sharp security suite—Technical questions & answers. Sharp Electronics Corporation, Sharp Plaza, Mahwah, NJ 07430-1163. www.sharpusa.com, www.sharpusa.com/security, documents provided to author.

Albert J. Marcella Jr., is president of Business Automation Consultants, LLC, a global information technology and management-consulting firm, established in 1984, to provide information technology (IT) management consulting and IT audit and security reviews and training for an international clientele. Dr. Marcella is an internationally recognized public speaker, researcher, workshop and seminar leader with over 30 years of experience in IT audit, security and assessing internal controls, and an author of numerous articles and 32 books on various IT, audit and security related subjects. Dr. Marcella's most recent book, Cyber Forensics: Collecting, Examining, and Preserving Electronic Evidence An Auditor's Field Manual, *second edition, focuses on issues, tools, and control techniques designed to assist audit, law enforcement, and info security professionals in the successful investigation of illegal activities perpetrated through the use of information technology. For additional information on the subject of cyber forensics contact Dr. Marcella at* amarcella@mindspring.com