Journal of Forensic & Investigative Accounting
Vol. 2, Issue 2

Technical, Legal and Internal Control Implications of Today's Digital Multifunctional Devices©

Al Marcella
Richard J. Dippel*

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.

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 internal auditor or 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.

A review of the major manufactures of photocopiers disclosed that the market although broad, is dominated by roughly 13 companies (Brother, Canon, Gestetner, IKON, Konica-Minolta, Okidata, Panasonic, Pitney Bowes, Ricoh, Savin, Sharp, Toshiba, and Xerox).

To investigate these photocopier brands as potential repositories of latent data, it is recommended that the auditor/investigator determine what, if any, potential exposures might exist with the overall security of the product.

One place to begin an assessment and to gather data on potential vulnerabilities is the National Vulnerability Database (NVD) (http://nvd.nist.gov). The NVD is a comprehensive

* The authors are, respectively, Professor and Assistant Professor, both at Webster University.

cyber security vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources. It is based on and synchronized with the Common Vulnerabilities and Exposures (CVE) vulnerability naming standard. The NVD is a product of the NIST Computer Security Division and is sponsored by the Department of Homeland Security's National Cyber Security Division.

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 CVE vulnerabilities. And it is the only vulnerability database that integrates Open Vulnerability Assessment Language (OVAL) queries.

CVE aspires to describe and name all publicly known facts about computer systems that could allow somebody to violate a reasonable security policy for that system. Often, these things are referred to as vulnerabilities.

The NVD statistics engine allows one to generate statistics on vulnerability trends over time. One can track particular products or vendors. Alternately, one can track sets of vulnerabilities with particular attributes (such as remotely exploitable buffer overflows).

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.

Security consultant Brendan O'Connor, states that "I cannot agree that the presence of more or less CVE listings for a given product or vendor is indicative of the security of said product(s). Just as Windows has more security vulnerabilities discovered than Mac OS (by an order of magnitude), it is not natively a more secure operating system.

It's just less widely used, therefore a much more attractive target. As Mac OS has become more popular in recent years, the amount of vulnerabilities discovered has also increased dramatically. I do not believe that Apple is currently writing less secure code than they were five or 10 years ago. I think vulnerability discovery is largely a function of the target system's popularity, not its quality or lack of quality from a security standpoint.

Just look at the iPhone for example. Its launch was surrounded by overwhelming hype and popularity, and the security industry attempted to find vulnerability in it as quickly as possible. There were actually cash rewards offered for the first person who found certain vulnerabilities. Is the iPhone then less secure than a blackberry, palm, or windows mobile device?"[1]

The National Vulnerability Database states "***One should consider not purchasing products that are showing to continually be vulnerable (especially those that have many high severity vulnerabilities).*** (Emphasis added by authors) (http://nvd.nist.gov/faq.cfm). O'Connor disagrees with this advice stating "I believe the core evolutionary principle that infection breeds immunity transfers to the software industry. Again, using Microsoft as an example, their current software has one of the lowest ratios of vulnerabilities per lines of code than any other software vendor. I think when one evaluates the security of a product or, especially, a vendor, one must consider several factors. These factors include mean time to vulnerability discovery, speed of vendor response (how quickly is a patch available, considering its complexity), and vendor reaction (do they come forward, or attempt to deny or bury it)."[1]

A "universal" vulnerability is one that is considered a vulnerability under any commonly used security policy which includes at least some requirements for minimizing the threat from an attacker. (This excludes entirely "open" security policies in which all users are trusted, or where there is no consideration of risk to the system (http://cve.mitre.org/about/terminology.html.).

An examination of entries for photocopier products in the NVD provided the following information:

- CVE-2006-6439. Xerox WorkCentre and WorkCentre Pro before 12.050.03.000, 13.x before 13.050.03.000, and 14.x before 14.050.03.000 allows remote attackers to download the audit log and obtain potentially sensitive information via unspecified vectors (12/10/2006).
- CVE-2006-6433. Xerox WorkCentre and WorkCentre Pro before 12.060.17.000, 13.x before 13.060.17.000, and 14.x before 14.060.17.000 does not record accurate timestamps, which makes it easier for remote attackers to avoid detection when an audit tries to rely on these timestamps (12/10/206).
- CVE-2006-4680. The Remote UI in Canon imageRUNNER includes usernames and passwords when exporting an address book, which allows context-dependent attackers to obtain sensitive information (9/11/2006, http://nvd.nist.gov/nvd).

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 NVD, prior to beginning a

forensic examination of a MFD may provide additional useful information for the auditor/investigator.

While the authors endeavored and ensured that the discussion of any products or services in this article remained free from specific vendor endorsement, the discussion of MFDs and their potential value (or exposure) to either an IT audit or a cyber forensic investigation, led to a simple, yet critical questions; "Can a photocopy machine be a potential source for latent electronic, forensic evidence? Should an auditor or investigator consider a MFD as a source of potential exposure, and risk to the disclosure of confidential data and breach of privacy (organizational or personal)?"

The short answer, most definitely "YES!"

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.

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 didn't know whether the device contained a hard drive.
- 65 percent said copier/printers presented little or no risk to data security.
- Five 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[2].

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. While IT and data security is not the primary

focus of this article, these issues and questions regarding controlling the potential exposure of MFDs will be addressed, albeit briefly, as appropriate throughout this article.

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. One vendor however, which stood out from the crowd in providing a potential security solution for exposed MFDs is Sharp Electronics (Sharp).

A review of the market for similar products and vendors proved futile and we came away empty. 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, Peter Cybuck, Associate Director Solution and Security Business Development at Sharp Electronics Corporation, was contacted. 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, Peter provided his insights, expertise and comments regarding the varied vulnerabilities associated with MFDs. Peter's sage advice is worth reading and re-reading by both the cyber forensics investigator and the professional charged with protecting his/her organization's data (e.g., internal auditors, IT security, etc.).

Please Note:

> *The authors, their estates and heirs yet to be born, oh you get the idea, are not endorsing products or services provided by this vendor. The vendor is referenced in an attempt to inform the reader and to call attention to a typically overlooked area which may require potential auditor and/or cyber forensic examination, as well as calling attention to a need to enhance existing corporate security protocols.*

Peter indicated that Sharp offers clients a solution in the form of a product called a Data Security Kit (DSK). This DSK is designed to protect document image data temporarily stored on

the hard drive, or in other memory, and data processed by the MFD during copy, scan, print or fax operations.

The DSK is an upgrade kit that not only adds security functions (e.g. encryption and overwrite) but also controls the major MFD systems and subsystems – print, copy, scan, fax jobs, network control, operating system, memory components (hard drive, RAM, ROM), local user interface, engine and job controller (including PostScript® and PCL).

Sharp's Data Security Kit offers multiple layers of security. First, all latent image data within the MFD is encrypted (using an AES algorithm) before being written to the hard drive, RAM or Flash memory.

Peter noted "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 (with the DSK product) up to seven times, rendering it unrecoverable[3].

"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" [4].

This point is both important to the auditor and cyber forensics investigator in that if a MFD is so protected, the potential of identifying and obtaining latent data is remote, and 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.

For the internal controls professional, the existence of such technology at the source is a significant control point, however, lack of such control features exposes the organization to potential catastrophic risk, legally as well as financially.

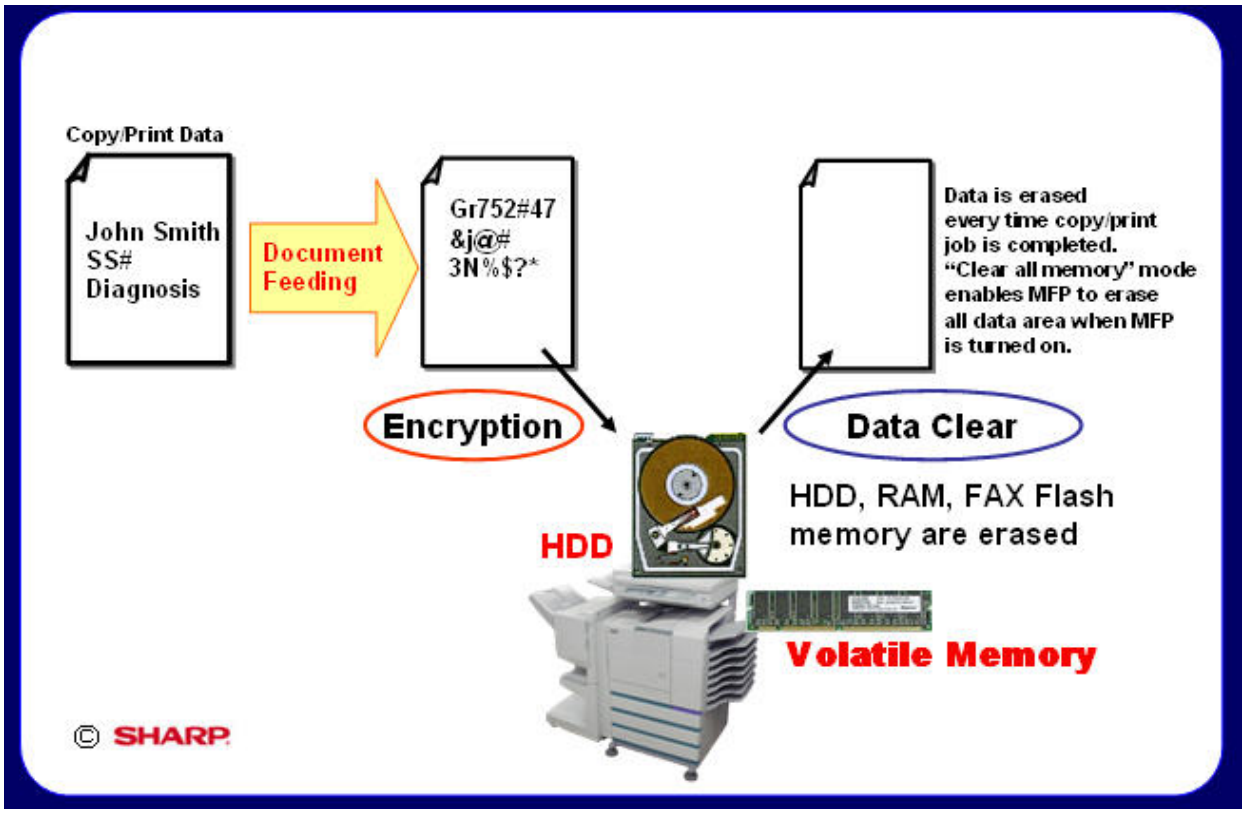

Figure 1 - Encryption and Data Clearing of Photocopied Material

Tackling the technology and the inherent process of the security potential surrounding the DSK product, security consultant O'Connor asks ". How is it possible to fully encrypt data before writing it to RAM? Input over the network (like a print job) is going to be read by the Ethernet driver and buffered in the IP stack. The packets must be clear text, otherwise nothing on the system could keep up with sequence numbers, perform CRCs, or know if requests were malformed."

Hypothetically, Sharp could have special NICs with their own set of RAM that encrypted the data at a hardware level, then handed it to the OS, but the NIC and the OS would need to have the same AES key. If they have the same key, how did they exchange it? It's in software somewhere.

Sharp has mention installing a "firmware upgrade" into the device when it is installed, so I'm assuming it's probably an ASIC for crypto. In their white papers, Sharp does not divulge any specifics on how this accomplished (security through obscurity). The OS on the device must be

able to interact with clear text data both in memory and on disk. Therefore, the OS must have knowledge of the key in order to function. Just as full disk encryption technologies encrypt the HD of a laptop, the OS itself sees everything as clear text."[1]

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 and government agencies 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."

A review of the NVD discloses….

> CVE-2006-6430. Web services in Xerox WorkCentre and WorkCentre Pro before 12.060.17.000, 13.x before 13.060.17.000, and 14.x before 14.060.17.000 do not require HTTPS, which allows remote attackers to obtain sensitive information by sniffing the unencrypted HTTP traffic (12/10/2006, http://nvd.nist.gov/nvd).

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[2].

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. With this in mind, this article isolates and examines what in the day was simply called a photocopy machine, i.e., the photocopier, and what is today referred to as an MFD. The once uni-task machine has grown up and grown into a multifunctional device hence the MFD, capable of not only photocopying an original document but also scanning, faxing, creating a PDF file and emailing that original to anyone with a valid email address, all from the same machine.

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).

Unlike corporate desk and laptops which over the past several years have received much attention when it comes to security, little if no attention has been afforded to securing data storage devices residing in corporate photocopiers, fax machines, etc. Why should this lack of security consideration over photocopiers and MFDs in general, be of concern, of interest, to a an auditor to a cyber forensic investigator? Read on.

The Technical Stuff

Most of the makes and models of today's photocopiers (a.k.a. MFDs) are outfitted with internal hard drives. These hard drives can range in size (storage capacity) from 40GB to much larger 80GB units. To put this in perspective, a 40MB hard drive is capable of storing/retaining:

- 43 billion characters
- 21 million pages of documents
- 374 feet of paper
- 838,000 pictures
- 16,384 songs

The same is true of the hard drive which resides in an organization's photocopier. In fact, a rough estimate of the storage capabilities of 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 emailed, 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, HIPAA, FERPA violation!).

Most copiers do not sequentially store the documents copied. If they did they would quickly run out of memory. Many over write 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[4].

Figure 2 - Vulnerability Points Resident in a MFD

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.

Security is number one because legislation has put the focus on privacy, and the new initiatives and product capabilities needed to assure compliance. Privacy laws are having an impact everywhere, so security-conscious organizations now make Information Assurance a priority for all products that process sensitive information.

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[5].

How the Process Works

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 don't realize is that the document information remains in the memory when they walk away from the machine.

Unlike previous generations of copiers, today's devices keep a copy of documents in memory, either on a hard drive, in RAM (Random Access Memory) or Flash memory. Just like a personal computer, the latent image data remains until that disk sector is overwritten. Documents could be accessed on the unit's hard drive from a PC and reprinted or the unit's hard drive could be replaced, moved or stolen[5].

The retained document data has unsettling ramifications for security-conscious organizations: It can expose confidential data to clever insiders and to enterprising cyber-thieves with enough savvy to hack into the machine's memory devices or penetrate its network interfaces.

Something as simple as moving your MFD to another department or selling it back to a broker after the lease expires, or taking it off site for repair or upgrade, all leave the hard disk, especially print mail boxes and controller hold and print queues exposed to data exposure and data theft. Fax data in flash memory is a similar concern. Residual confidential document data can remain in memory years after a print or copy job is completed.

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[6].

Knowledge of how this procedure works is a critical asset to both the auditor and the cyber forensic investigator and to his/her efforts in conducting a thorough audit/investigation and ensuring that all potential sources of electronic forensic evidence are examined.

Digital copiers store thousands of records in internal memory. At the end of a copier's lease period, thousands of records retained on the hard drive can fall into the wrong hands…this poses a privacy compliance risk.

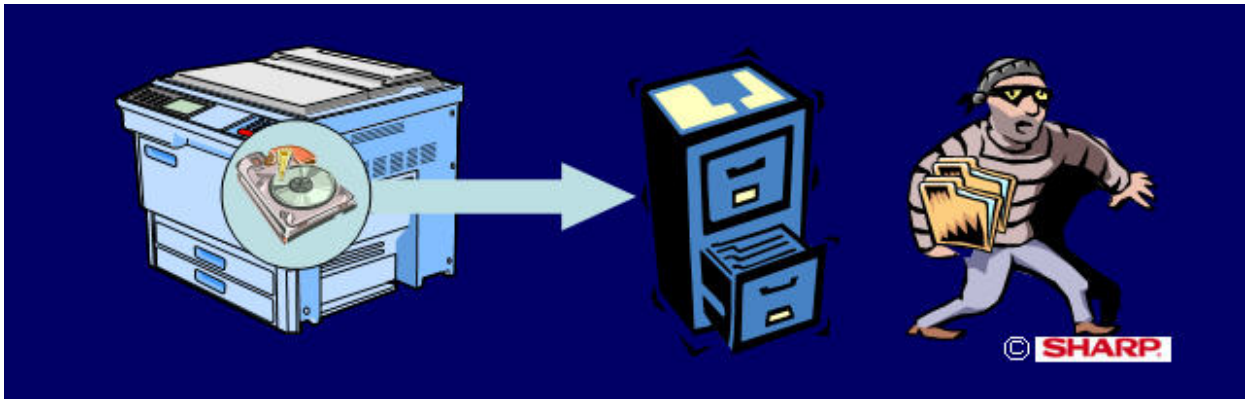

Figure 3 - Privacy and Compliance Risks Inherent Within MFDS

The Forensic Application

For most organizations, the more serious threat to data security does not come from external sources but, from internal sources, employees, contractors who come to work, have access to the building, systems, applications and ultimately data, sensitive, valuable, critical data. Recent reports from the FBI point to internal threats as often being the greatest point of exposure for an organization.

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[5].

Ted, a mid-level manager supervises several engineers in his company's R&D department. Sally, a vendor's rep, an entrepreneurial business woman, convinces Ted to sell her schematics and blueprints for a new hydraulic press Ted's company is developing. Excited by the potential for financial gain, Ted agrees, however, he does not want to get caught with paper or electronic copies of the documents either on his person or his desktop workstation.

Ted, staying late one evening, simply goes to the company's photocopier and selects the scan and email options and in a matter of mere minutes (possibly seconds), copies, scans and emails the schematics and blueprints, saved as a PDF formatted file to Sally. Ted meets Sally, receives his payment and agrees to send Sally additional proprietary documents as they become available.

Alerted by a competitor to whom Sally attempted to sell the documents, Ted's company launches an investigation into the "leak". As part of the investigation Ted's computer is seized and a audit/cyber forensic examination in preformed on Ted's computer. No incriminating evidence is uncovered as a result of the investigation.

It is at this point that the auditor/cyber forensic examiner may elect to expand the scope of the investigation to include an examination of other data storage devices to which Ted may have had access. Prior to reading this article, would you have considered auditing the office photocopy machine? Would you – seriously? I hope that now you will!!

Legal Issues

There are numerous federal statutes and both federal and state court decisions that recognize claims based on a breach of the right to privacy or invasion of privacy. In addition, physicians (Section 5.05 of the AMA Code of Ethics), attorneys (Rule 1.6 of the ABA Model Rules of Professional Conduct) and accountants (Rule 301 of the AICPA Code of Professional Conduct) have a professional responsibility to maintain confidentiality of client information. Also, confidentiality can be an aspect of a contractual agreement.

Some of the federal statutes involving the right to privacy include the Cable Communications Policy Act, 47 U.S.C. Section 551 (1984), Driver's Privacy Protection Act, 18 U.S.C. Section 2721 (1994), Fair Credit Reporting Act (FCRA), 15 U.S.C. Section 1681 et. seq. (1970), Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. Section 1232g (1974), Gramm-Leach-Bliley Act (GLB), 15 U.S.C. Section 6801 et. seq. (1999), Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. Section 1320d et. seq. (1996) and Privacy Act, 5 U.S.C. Section 552a (1974).

The various laws and court decisions involve criminal penalties and civil damages based on the responsibility of the defendant for the disclosure of private information. A review of penalties of the HIPAA includes civil penalties of money damages and criminal penalties of fines and imprisonment (42 U.S.C. Sections 1320d-5 and 1320d-6). The criminal penalties in HIPAA result from intentional acts and the civil damages result from violation of the act that does not require intentional acts.

State court decisions in many states have fashioned a right to privacy under state law under the cause of action known as "invasion of privacy". The United States Court of Appeals for the Eighth Circuit, in *Ruzicka Elec. & Sons, Inc. v. IBEW*, 427 F.3d 511, 535 (8th Cir. 2005), stated that in order to make a case for invasion of privacy, the plaintiff must prove the existence of private subject matter, a right of the plaintiff to keep the matter secret and that the obtaining of the information by the defendant was in an objectionable manner. In *Bratt v. Int'l Business*

Machines Corp., 785 F.2d 352 (1st Cir. 1986), the court used a balancing test between the level of intrusion and the employer's interests.

In a footnote to a DePaul University Business Law Journal article, the author of the article raised the possibility of a negligent maintenance of records theory of recovery. *Invasion of Privacy: Refocusing the Tort in Private Sector Employment*, 6 DePaul Bus. L.J. 41 (1994). This footnote was supported by several reported cases including an Illinois appellate court decision.

Therefore, these statutes and court decisions evidence expanded liability based on negligence, reckless or intentional conduct that can result in liability for the MIS-handling of private information. The imposition of the doctrine of respondeat superior [Latin for "let the master answer" is a legal doctrine which states that, in many circumstances, an employer is responsible for the actions of employees performed within the course of their employment] where the negligence acts of the employee, within the scope of employment, can create liability for the company. In addition, cases involving the liability of businesses in the context of employment discrimination could be an indicator of the exposure of business to cases involving an intentional breach of privacy.

In *Durham Life Ins. Co. v. Evans*, 166 F.3d 139 (3rd Cir 1999), the court in a discrimination case in citing a Supreme Court case, indicated that an employer could be liable for behavior prohibited by the company because such behavior is aided by the manager's overall agency relationship with the company. In *Russell v McKinney Hosp. Venture*, 235 F.3d 219, 226 (5th Cir. 2000), the persons committing the improper activity was determined to have influence over a manager's actions in the company resulting in liability for the company.

Consequently, the failure to recognize and protect against a breach of privacy in the context of the use of copiers or multifunctional machines can expose a company to liability based on the protections afforded to individuals by federal and state statutes and federal and state court decisions.

Professionals such as physicians, attorneys and accountants are also at risk, as are public and private companies, state and private academic institutions. Further, companies that are contractually obligated to maintain confidential records are also at risk. In addition, please note that unlike federal laws such as HIPAA, which has limits on the damages and penalties assessed, claims under the state laws can be without limits. Accordingly, it is essential that companies

must secure the use of such devices by instituting a strong set of internal controls and must ensure that information contained in such devices are protected from access by third parties.

Assessing the MFD Exposure

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 forensically audit the hard drives of suspect MFDs.

It should be noted that even if the MFD has marginal security, or if it is very secure, it may be impossible for the auditor/investigator to obtain sufficient electronic evidence which would proved, beyond question, that Ted actually photocopied and emailed proprietary documents to an external third party.

The Examination Process

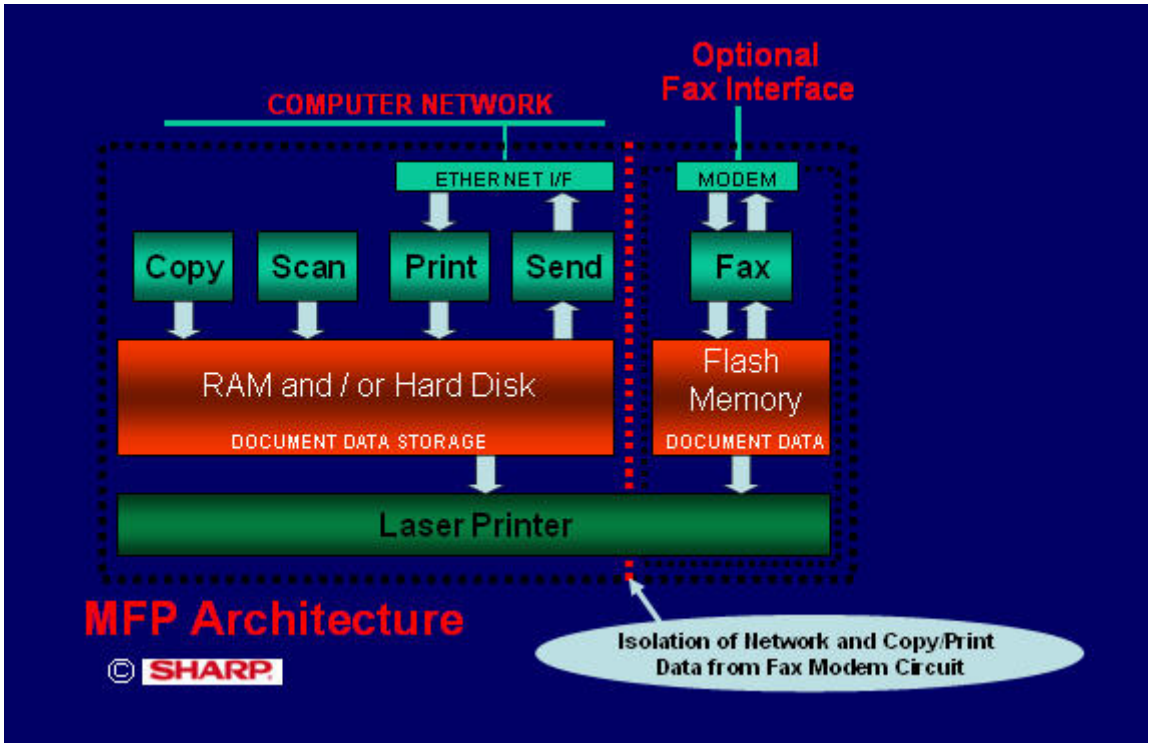

Figure 4 - Isolation of Network and Copy/print Data from Fax/Modem Circuit

Presented with the question, "How exactly would an auditor or a cyber forensic investigator access stored images retained on the 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.
>
> Vendors who incorporate soft operating systems in their MFDs will most likely have potential security vulnerabilities associated with their MFDs. An examination of the NVD for the vendor's MFD under investigation (as discussed earlier) is a valuable exercise."

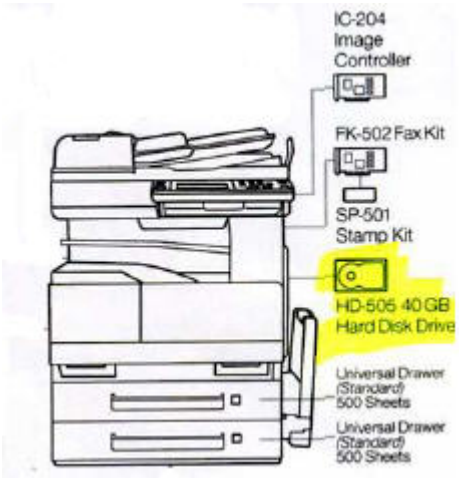

Figure 5 - MFD's Hard Drive Location

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 electronic evidence, there is no guarantee that said evidence will be useable, lead to a convection, 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 send the purloined PDF attached email to Sally.

Consider for a moment, the example of someone printing confidential information from company records since that information may be the easiest to recover. Stored fax pages and print files are usually the easiest to recover. The FBI report on Hansen the convicted FBI spy showed that he used the FBI's office copier to copy and print classified documents that he simply stuffed in his briefcase, and as a trusted, authorized insider, simply walked out of the building.

If the electronic evidence gathered by the auditor/investigator can not place Ted at the MFD, as the individual who sent the scanned PDF email to Sally, and is unable to obtain any additional corroborating evidence which can be substantiated or forensically verified, the organization may never be able to prove, beyond a doubt, that Ted was the individual responsible for sending Sally the schematics.

Implementation of specific security features such as Sharp's DSK, 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"[4].

Summary

The auditor or the cyber forensic investigator should conduct an initial "inventory" of data storage devices accessible by the subject of the investigation, to establish a pool of potential devices which may require detailed forensic examination.

Today's MFDs pose a considerable risk in the unsecured data which may be accessible to unauthorized individuals, violating such legislation as FERPA, HIPAA, GLB, etc., 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. Cybuck states that "Sharp's use of encrypted PDFs addresses this issue."

Today's 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 authors wishes to personally thank Peter Cybuck and Brendan O'Connor for their valuable time in discussing security issues related to uncontrolled MFDs and to provide their insights and expertise on the subject of MFDs and their potential exposures and the role MFDs play in an IT audit or cyber forensic investigation. Readers interested in obtaining further information regarding Sharp's DSK product may find additional information at www.sharpusa.com/security.

The underlying basis for this article (excluding the legal issues section) is taken from Dr. Marcella's book Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, second edition, the material is used with permission of the publisher Taylor & Francis Group, ISBN 0-84938-328-5.

REFERENCES

O'Connor, B. (January 2008). Personal correspondence with authors.

Cybuck. P. (2003),"Machine Talk: What secrets are your office equipment passing along?", Security Products, page 34, March 2003, retrieved March 2007.

Sharp Electronics Corporation, (December 2006), "Sharp Security Suite – Technical Questions & Answers," Sharp Electronics Corporation Sharp Plaza, Mahwah, NJ 07430-1163 1-800-BE-SHARP, www.sharpusa.com, www.sharpusa.com/security, documents provided to authors.

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 1-800-BE-SHARP, www.sharpusa.com, documents provided to authors.

Cybuck, P. (May 2005), "Accountable for Security," Feature Interview, Sharp Electronics Corporation Sharp Plaza, Mahwah, NJ 07430-1163 1-800-BE-SHARP www.sharpusa.com, www.ipac.ca, documents provided to authors.

The opinions of the authors are not necessarily those of Louisiana State University, the E.J. Ourso College of business, the LSU Accounting Department, Roosevelt University, the Senior Editor, or the Editor.