Advanced Corporate Solutions

"Debugging" Specialists | Service Excellence since 1995

DIGITAL PHOTOCOPIER MACHINES

Federal Trade Commission, United States of America, July 2017

DIGITAL PHOTOCOPIERS DATA SECURITY: A GUIDE FOR BUSINESSES

https://www.ftc.gov/tips-advice/business-center/guidance/digital-copier-data-security-guide-businesses

Does your company keep sensitive data — Social Security numbers, credit reports, account numbers, health records, or business secrets? If so, then you've probably instituted safeguards to protect that information. Your information security plans also should cover the digital copiers your company uses. If the data on your copiers gets into the wrong hands, it could lead to fraud and identity theft.

DIGITAL COPIERS ARE COMPUTERS

Today’s generation of networked multifunction devices — known as “digital copiers” — are “smart” machines that are used for more than just copying; they can do everything from copying, printing, scanning, faxing to emailing documents. Digital copiers require hard disk drives to manage incoming jobs and workloads, and to increase the speed of production.

The hard drive in a digital copier stores data about the documents it copies, prints, scans, faxes or emails. If you don’t take steps to protect that data, it can be stolen from the hard drive, either by remote access or by extracting the data once the drive has been removed.

THE LIFE-CYCLE OF A COPIER

Digital copiers often are leased, returned, and then leased again or sold. It’s important to know how to secure data that may be retained on a digital copier hard drive, and what to do with a hard drive when you return a leased copier or dispose of one you own. It’s wise to build in data security for each stage of your digital copier’s life-cycle: when you plan to acquire a device, when you buy or lease, while you use it, and when you turn it in or dispose of it.

Before you acquire a copier:

Make sure it’s included in your organization’s information security policies. Copiers should be managed and maintained by your organization’s IT staff. Employees who have expertise and responsibility for securing your computers and servers also should have responsibility for securing data stored on your digital copiers. Consider how your digital copier will need to be configured to comply with your organization’s information security. Copiers may have multiple network connections, including wifi, that will need to be secured like other wifi capable devices in your network.

When you buy or lease a digital copier:

Evaluate your options for securing the data on the device. Most manufacturers offer data security features with their digital copiers, either as standard equipment or as optional add-on kits. Typically, these features involve encryption and overwriting.

Encryption scrambles the data on the hard drive so it can be read only by particular software. Digital copiers that offer encryption encode the data stored on the hard drive so that it cannot be retrieved even if the hard drive is removed from the machine.

Overwriting — also known as file wiping or shredding — changes the values of the bits on the disk that make up a file by overwriting existing data with random characters. By overwriting the disk space that the file occupied, its traces are removed, and the file can't be reconstructed as easily.

Depending on the copier, the overwriting feature may allow a user to overwrite after every job run, periodically to clean out the memory, or on a preset schedule. Users may be able to set the number of times data is overwritten — generally, the more times the data is overwritten, the safer it is from being retrieved. However, for speed and convenience, some printers let you save documents (for example, a personnel leave slip) and print them straight from the printer hard drive without having to retrieve the file from your computer. For copiers that offer this feature, the memory is not overwritten with the rest of the memory. Users should be aware that these documents are still available. Overwriting is different from deleting or reformatting. Deleting data or reformatting the hard drive doesn't actually alter or remove the data, but rather alters how the hard drive finds the data and combines it to make files: The data remains and may be recovered through a variety of utility software programs. Yet another layer of security that can be added involves the ability to lock the hard drives using a passcode; this means that the data is protected, even if the drive is removed from the machine. Finally, think ahead to how you will dispose of the data that accumulates on the copier over time. Check that your lease contract or purchase agreement states that your company will retain ownership of all hard drives at end-of-life, or that the company providing the copier will overwrite the hard drive.

When you use the copier:

Take advantage of all its security features. Securely overwrite the entire hard drive at least once a month.

If your current device doesn't have security features, think about how you will integrate the next device you lease or purchase into your information security plans. Plan now for how you will dispose of the copier securely. For example, you may want to consider placing a sticker or placard on the machine that says: "Warning: this copier uses a hard drive that must be physically destroyed before turn-in or disposal." This will inform users of the security issues and remind them of the appropriate procedures when the machine reaches the end of its usable life.

In addition, your organization's IT staff should make sure digital copiers connected to your network are securely integrated. Just like computers and servers that store sensitive information, networked copiers should be protected against outside intrusions and attacks.

Use authentication at the device. In other words, require a password, card swipe, biometric information, or other authentication when physically accessing the device. Consider using "pull printing" — which is sometimes called "walk-up printing" and "release printing" – if your digital copier manufacturer offers it. Pull printing is software that stores documents you intend to print, but before the job will print, the user must supply proof of his or her identity. You can also use software to create rules to manage print jobs. Use these print rules to restrict access to certain printers and to provide audit trails to help determine culpability in the event of a breach.

Change the default network password.

When you finish using the copier:

Check with the manufacturer, dealer, or servicing company for options on securing the hard drive. The company may offer services that will remove the hard drive and return it to you, so you can keep it, dispose of it, or destroy it yourself. Others may overwrite the hard drive for you. Typically, these services involve an additional fee, though you may be able to negotiate for a lower cost if you are leasing or buying a new machine. One cautionary note about removing a hard drive from a digital copier on your own: hard drives in digital copiers often include required firmware that enables the device to operate. Removing and destroying the hard drive without being able to replace the firmware can render the machine inoperable, which may present problems if you lease the device. Also, hard drives aren't always easy to find, and some devices may have more than one. Generally, it is advisable to work with skilled technicians rather than to remove the hard drive on your own.

Protecting Sensitive Information: Your Legal Responsibility

The FTC's standard for information security recognizes that businesses have a variety of needs and emphasizes flexibility: Companies must maintain reasonable procedures to protect sensitive information. Whether your security practices are reasonable depends on the nature and size of your business, the types of information you have, the security tools available to you based on your resources, and the risks you are likely to face. Depending on the information your business stores, transmits, or receives, you also may have more specific compliance obligations. For example, if you receive consumer information, like credit reports or employee background screens, you may be required to follow the Disposal Rule, which requires a company to properly dispose of any such information stored on its digital copier, just as it would properly dispose of paper information or information stored on computers. Similarly, financial institutions may be required to follow the Gramm-Leach-Bliley Safeguards Rule, which requires a security plan to protect the confidentiality and integrity of personal consumer information, including information stored on digital copiers.

FOR MORE INFORMATION

To learn more about securing sensitive data, in general, read Protecting Personal Information: A Guide for Business at https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security.

NEW YORK, April 15, 2010

DIGITAL PHOTOCOPIERS CAN BE LOADED WITH SECRETS

http://www.cbsnews.com/stories/2010/04/19/eveningnews/main6412439.shtml
(link no longer available)

YOUR OFFICE COPY MACHINE MIGHT DIGITALLY STORE THOUSANDS OF DOCUMENTS THAT GET PASSED ON AT RESALE

This year marks the 50th anniversary of the good, old-fashioned copy machine. But, as Armen Keteyian reports, advanced technology has opened a dangerous hole in data security. John Juntunen's company Digital Copier Security - developed software that can scrub all the data on photocopier hard drives.

Modern office photocopiers with a hard drive could pose a security risk for those who use them.

At a warehouse in New Jersey, 6,000 used copy machines sit ready to be sold. CBS News chief investigative correspondent Armen Keteyian reports almost every one of them holds a secret.

Nearly every digital copier built since 2002 contains a hard drive - like the one on your personal computer - storing an image of every document copied, scanned, or emailed by the machine. In the process, it's turned an office staple into a digital time-bomb packed with highly personal or sensitive data. If you're in the identity theft business, it seems this would be a pot of gold.

"The type of information we see on these machines with the social security numbers, birth certificates, bank records, income tax forms" John Juntunen said, "is information that would be very valuable."

Juntunen's Sacramento-based company, Digital Copier Security, developed software called "INFOSWEEP" that can scrub all the data on hard drives. He's been trying to warn people about the potential risk - with no luck. "Nobody wants to step up and say, "We see the problem, and we need to solve it,'" Juntunen said. This past February, CBS News went with Juntunen to a warehouse in New Jersey, one of 25 across the country, to see how hard it would be to buy a used copier loaded with documents. It turns out ... it's pretty easy.

Juntunen picked four machines based on price and the number of pages printed. In less than two hours his selections were packed and loaded onto a truck. The cost? About $300 each. Until we unpacked and plugged them in, we had no idea where the copiers came from or what we'd find. We didn't even have to wait for the first one to warm up. One of the copiers had documents still on the copier glass, from the Buffalo, N.Y., Police Sex Crimes Division.

It took Juntunen just 30 minutes to pull the hard drives out of the copiers. Then, using a forensic software program available for free on the Internet, he ran a scan - downloading tens of thousands of documents in less than 12 hours. The results were stunning: from the sex crimes unit there were detailed domestic violence complaints and a list of wanted sex offenders. On a second machine from the Buffalo Police Narcotics Unit we found a list of targets in a major drug raid.

The third machine, from a New York construction company, spit out design plans for a building near Ground Zero in Manhattan; 95 pages of pay stubs with names, addresses and social security numbers; and $40,000 in copied checks.

But it wasn't until hitting "print" on the fourth machine - from Affinity Health Plan, a New York insurance company, that we obtained the most disturbing documents: 300 pages of individual medical records. They included everything from drug prescriptions, to blood test results, to a cancer diagnosis. This is a potentially serious breach of federal privacy law. "You're talking about potentially ruining someone's life," said Ira Winkler, "Where they could suffer serious social repercussions."

Winkler is a former analyst for the National Security Agency and a leading expert on digital security. "You have to take some basic responsibility and know that these copiers are actually computers that need to be cleaned up," Winkler said.

The Buffalo Police Department and the New York construction company declined comment on our story. As for Affinity Health Plan, they issued a statement that said, in part, "We are taking the necessary steps to ensure that none of our customers' personal information remains on other previously leased copiers, and that no personal information will be released inadvertently in the future."

Ed McLaughlin is President of Sharp Imaging, the digital copier company. "Has the industry failed, in your mind, to inform the general public of the potential risks involved with a copier?" Keteyian asked. "Yes, in general, the industry has failed," McLaughlin said.

In 2008, Sharp commissioned a survey on copier security that found 60 percent of Americans "don't know" that copiers store images on a hard drive. Sharp tried to warn consumers about the simple act of copying. "It's falling on deaf ears," McLaughlin said. "Or people don't feel it's important, or 'we'll take care of it later.'"

All the major manufacturers told us they offer security or encryption packages on their products. One product from Sharp automatically erases an image from the hard drive. It costs $500. But evidence keeps piling up in warehouses that many businesses are unwilling to pay for such protection, and that the average American is completely unaware of the dangers posed by digital copiers.

The day we visited the New Jersey warehouse, two shipping containers packed with used copiers were headed overseas - loaded with secrets on their way to unknown buyers in Argentina and Singapore.