

Risk Monitor



Copy Machines: A Prime Identity Theft Target

It is hard to believe that the copy machine just recently celebrated its 50th birthday. There's no question that these popular technological devices have proven to be worth their weight in gold for countless consumers and businesses. From copying to scanning and even emailing documents, copy machines are a must-have for most modern day companies.

However, there's a secret lurking inside the common copy machine that has identity thieves across the nation salivating. Nearly every copier that was built since 2002 includes a hard drive. This relatively small unit, hidden inside the copy machine, stores an image of every single document scanned or copied by the machine.

An identity thief's dream

Most copiers store up to 20,000 document images, which often include Social Security numbers, birth certificates, bank records, income tax forms, medical records and other valuable information. In other words, these hard drives contain the type of data that identity thieves are itching to get their hands on.

Perhaps even more frightening is this fact: Anyone can easily buy used copiers from office supply vendors. Oftentimes, a used copier that initially cost thousands of dollars is sold for just \$300 or less. Quite a few vendors sell these used copiers to overseas buyers.

Most sellers do not erase the hard drive before selling a used copier. That means the buyer gains immediate access to all the

invaluable information stored on the hard drive for just a few hundred bucks. With a special device, an identity thief can easily scan and download all the document images stored on this hard drive.

However, an identity thief doesn't even have to buy the copier to gain access to the profitable data inside. He could simply hack into the office copier's hard drive to get his hands on the wealth of information stored there.

Understanding the risks

Unfortunately, most of the general public is completely unaware of the potential risks associated with copy machines. A recent study revealed that 60 percent of Americans do not even realize that copiers store images on a hard drive.

Luckily, there are ways to combat the threat of identity thieves stealing data from copy machines. Some copy machine security companies have the ability to "scrub" or delete all of the info on copy machine hard drives before a business gets rid of the copier.

Additionally, some new copy machine models include a feature allowing users to automatically erase images from the copier's hard drive. This extra feature typically costs about \$500. It could be worth the added expense. Af-

ter all, this feature could end up saving you thousands of dollars in identity theft damages.



Welcome to The Chadler Group's Newsletter!

It is with great satisfaction that we bring our newsletter to you. In this issue and the coming quarterly newsletters, we will discuss pertinent insurance topics which affect your business and personal insurance needs. We hope you find this information both informative and useful in your overall risk management practices.



The Chadler Group, Inc.
PO Box 11115
330 Passaic Ave, Ste. 200
Fairfield, NJ 07004

Phone: (800) 706-2478
Fax: (973) 227-4026



Seven Ways Your Business Can Prevent Cybercrime

Legendary bank robber Willie Sutton supposedly said that he robbed banks because that was where the money was. Many small business owners follow this logic when it comes to computer system security. They believe that people who rob with a mouse and a keyboard rather than a gun target large corporations, because those businesses have the most money. This leads them to the misguided belief that cybercriminals will not bother them. In fact, the NACHA - The Electronic Payments Association - reports that Eastern European criminal syndicates have targeted small businesses precisely because they have allowed themselves to become easy marks.

Experts in the field estimate that one in five small businesses do not use antivirus software, 60 percent do not encrypt data on their wireless networks, and two-thirds lack a data security plan. This failure to take precautions makes a small business easy pickings for computer hackers. However, there are several things business owners can do to protect themselves.

1. Use two-factor authentication. This is a mechanism that requires the user to do more than one thing for authentication. It ordinarily has two components -- one thing the user knows (such as a password), the other a randomly generated number that the user must input. The number comes from an electronic token card, which generates a new number every few seconds. If the user enters a number that the system is expecting, the system will authenticate the user.
2. Inoculate systems against the Clampi Trojan virus. This virus resides on a computer, waiting for the user to log onto financial websites. It captures log-in and password information, relays it to servers run by the criminals, instructs the computer to send money to accounts that they control, or steals credit card information and uses it to make unauthorized purchases. The trojan monitors more than 4,500 finance-related websites.
3. Be on guard against "phishing" e-mails and pop-up messages. These messages purport to be from legitimate businesses with which the recipient does business. They ask the user to update or verify information, often threatening negative consequences if she fails to do so. Clicking on the links in the messages brings the user to an authentic looking Web site. However, it is actually bogus; the site collects personal information that the collector can use to steal the user's identity. System users should ignore these messages.
4. Arrange for financial institutions to alert the business owner should they spot unusual activity involving the firm's accounts.
5. Install firewalls and encryption technology to block uninvited visitors from uploading to or retrieving data from the

firm's servers and to protect data sent on public networks. Intrusion detection systems can inform the business owner of attempts to hack into the network.

6. Be cautious about opening attachments to e-mails, especially if the sender is someone unfamiliar to the user. Attachments may contain viruses or Trojan horses that can steal login information and passwords or corrupt a system.



7. Protect against intrusion by disgruntled former or current employees. Deactivate passwords for former employees, erect barriers to keep employees from accessing systems unrelated to their jobs, and implement sound accounting procedures for financial transactions.

In addition to these safeguards, small businesses may want to consider purchasing computer fraud and employee theft insurance. These policies will protect the business against those losses that still occur; insurance companies are likely to offer favorable pricing to businesses that take precautions against cybercrime. A professional insurance agent can give advice on the appropriate types and amounts of coverage.

Modern technology gives businesses unprecedented abilities, but it also presents significant risks. Every business owner must take steps to keep the cybercriminals out.



Steps to Reduce Credit Card Fraud

Credit card fraud has blossomed in the past decade. By becoming vigilant in recognizing the red flags and taking proactive measures you can substantially reduce potential credit card fraud for your business.

Credit card fraud occurs in two primary areas:

- On the business premises
- Through internet and phone purchases

As both situations are different, there are several different strategies you can use to protect yourself.

Business Premises

Personal interaction with your customers allows for better credit card fraud management for the following reasons:

- Set purchase limits before identification is required. Train employees to examine the types of purchases as smart fraudsters will try to stay under these purchase limits.
- Examine picture identification. Remember to always scrutinize the identification to look for signs the picture ID was altered.
- Visually inspect the credit card itself, especially hologram features which many credit card companies now employ and which are very difficult to duplicate. If the hologram image does not move when you slant the card this is a definite red flag.
- Compare the credit card number with lists of fraudulent or stolen credit card numbers.
- Visually inspect the signature on the credit card receipt and compare it to signatures on the receipt to see whether the credit card signature was altered. The signature panel on most cards today has duplicate color designs of the credit card company name. Fraudsters will often try to tape over the original signature and apply their own.
- Examine the raised credit card numbers and name on the card to look for 'ghost' or smear images. Any apparent defect should be treated with suspicion.
- Call the credit card company to confirm that large purchases will be authorized by the credit card company.

- Set a specific procedure to ensure that all duplicate copies of credit cards receipts are properly destroyed.

Internet and Phone Purchases

Indicators of credit card fraud and safeguards you can employ for phone and Internet purchases include:

- Ensuring you request sufficient contact information from customers including phone numbers and both mailing and billing addresses.
- A rush order is the most popular preference of credit card fraudsters.
- Purchases which are initiated from a 'free' e-mail address or which employ a forwarding e-mail address should be considered highly suspicious. Ensure that you obtain an IP address or an e-mail address which has a domain so you can track the buyer.
- Be especially cautious about orders that appear larger than normal or are purchased with more than one credit card or several cards where the numbers follow in a sequence.
- Obtain phone contact information if the billing address is not the same as the shipping address, especially if it's a P.O. Box number.
- Carefully scrutinize all order forms and never fill any order where the order information is incomplete.
- Take caution with overseas shipping and especially if any of the above criteria occurs. Certain geographic areas such as Eastern Europe, Africa, Malaysia, Indonesia, Turkey, and Pakistan are considered high risk where overseas sales are concerned.
- Where possible, use an address verification system and always confirm the screening process if you use a payment gateway system.
- Don't hesitate to contact the credit card company if you have doubts.
- Don't be reticent to even ask the customer to mail some form of photo ID for expensive items or large orders.
- Clearly indicate your credit screening process on your web site.

continued from page 4...Is It Legal for You to Obtain Your Employee's MVR?

Some employers ask their insurance agents to obtain employees' driving records. The DPPA permits agents to order these records for insurance purposes and allows a person with a permissible use to share information with another person with a permissible use. The FCRA, however, imposes on the agent the same obligations that a consumer reporting agency would have. In addition, some vendors forbid agents from sharing the records.

Businesses have a legitimate need for some information about how their employees drive. Employees have an equally legitimate concern about who will see their information and how it will be used. These laws attempt to balance business needs and employee privacy rights. All employers should familiarize themselves with these laws and state laws that may restrict their access to personal information.

Is It Legal for You to Obtain Your Employee's MVR?

Employers frequently require their workers to drive on company business. For some firms, driving may be the major part of employees' jobs. Other companies may need salespeople or inspectors to drive as an incidental but necessary part of their jobs. Even companies that perform most of their work in an office will need employees to drive at least occasionally to projects, conferences, or job sites. Employers who require their employees to do driving at all take the risk that their workers will become involved in automobile accidents. These incidents subject employers to medical bills, the costs of repairing or replacing damaged vehicles and property, and potential lawsuits from third parties.

Employers can get a fair picture of how employees drive by obtaining copies of their employees' motor vehicle records (MVR). Employers who decide to do obtain their employees' MVRs need to be aware of the boundaries set by federal and state laws.

Congress enacted the Driver's Privacy Protection Act (DPPA) of 1994 to restrict access to personal information that may appear on an individual's driving record. Personal information is anything that can identify a person, such as a name, photograph, Social Security number, phone number, address, or similar information. The law allows a motor vehicle bureau to release the record, including personal information, to anyone who has a permissible use. There are 14 permissible uses; three are relevant

to employers. A bureau may disclose information for use in the normal course of business to verify the accuracy of personal information a person provided to the business and, if the information is inaccurate, to obtain accurate information to prevent fraud. Also, an employer may obtain information relating to the holder of a commercial driver's license. Any person may obtain another's MVR if he can show a written consent by the other party for its release.

The federal Fair Credit Reporting Act (FCRA) is more restrictive. This law governs the release of consumer reports, a term that includes driving records, credit reports, credit scores, and others. It provides that a consumer reporting agency (such as Equifax) may not release a consumer record to an employer for employment purposes unless the consumer has given written permission. Therefore, a messenger service that wants to look at prospective employee Bob's driving record before hiring him must get Bob's written permission first. The consumer reporting agency must give Bob a Summary of Consumer Rights. If the employer takes an adverse action against Bob (doesn't hire him, declines to promote him, etc.) at least in part because of the information in his report, it must give him a Notice of Adverse Action, advising him of the information that affected the decision and the name of the reporting agency.

continued on page 3



The Chadler Group, Inc.
PO Box 11115
330 Passaic Ave, Ste. 200
Fairfield, NJ 07004

Phone: (800) 706-2478
Fax: (973) 227-4026

Risk Monitor