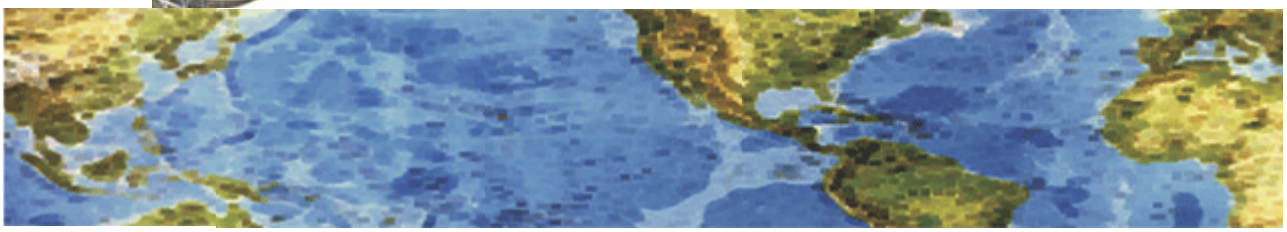
HALL ASSOCIATES



Risk-Based Decision Making Commentary
September 2012 Newsletter #3

Copier Data Security: A Guide for Businesses by the FTC

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, whether it's stored in computers or on paper. That's not only good business, but may be required by law. According to the Federal Trade Commission 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.

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. Digital copiers store different types of information in different ways. For example, photocopied images are more difficult to access directly from the hard drive than documents that are faxed, scanned or printed on the copier.

If 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. When you buy or lease a copier evaluate your options for securing the data on the device. Most manufacturers offer data security features with their copiers, either as standard equipment or as optional add-on kits.

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.

http://business.ftc.gov/documents/bus43-copier-data-securityis a link to the full article.

HALL ASSOCIATES

FTC Halts Computer Spying

Secretly Installed Software on Rented Computers Collected Information, Took Pictures of Consumers in Their Homes, Tracked Consumers' Locations

Seven rent-to-own companies and a software design firm have agreed to settle Federal Trade Commission charges that they spied on consumers using computers rented from them, capturing screenshots of confidential and personal information, logging their computer keystrokes, and in some cases taking webcam pictures of people in their homes, all without notice to, or consent from, the consumers. The software design firm collected the data that enabled rent-to-own stores to track the location of rented computers without consumers' knowledge. The settlements bar the companies from any further illegal spying, from activating location-tracking software without the consent of computer renters and notice to computer users, and from deceptively collecting and disclosing information about consumers.

"An agreement to rent a computer doesn't give a company license to access consumers' private emails, bank account information, and medical records, or, even worse, webcam photos of people in the privacy of their own homes," said Jon Leibowitz, Chairman of the FTC. "The FTC orders today will put an end to their cyber spying." The FTC named DesignerWare, LLC, a company that licensed software to rent-to-own stores to help them track and recover rented computers. The FTC also reached settlements with seven companies that operate rent-to-own stores and licensed software from DesignerWare, including franchisees of Aaron's, ColorTyme, and Premier Rental Purchase.

According to the FTC, DesignerWare's software contained a "kill switch" the rent-to-own stores could use to disable a computer if it was stolen, or if the renter failed to make timely payments. DesignerWare also had an add-on program known as "Detective Mode" that purportedly helped rent-to-own stores locate rented computers and collect late payments. DesignerWare's software also collected data that allowed the rent-to-own operators to secretly track the location of rented computers, and thus the computers' users. When Detective Mode was activated, the software could log key strokes, capture screen shots and take photographs using a computer's webcam, the FTC alleged. It also presented a fake software program registration screen that tricked consumers into providing their personal contact information. Data gathered by DesignerWare and provided to rent-to-own stores using Detective Mode revealed private and confidential details about computer users, such as user names and passwords for email accounts, social media websites, and financial institutions; Social Security numbers; medical records; private emails to doctors; bank and credit card statements; and webcam pictures of children, partially undressed individuals, and intimate activities at home, according to the FTC.

The seven rent-to-own companies were charged with breaking the law by secretly collecting consumers' confidential and personal information and using it to try to collect money from them. Use of the bogus "registration" information was deceptive, the FTC alleged.
http://www.ftc.gov/opa/2012/09/designware.shtm is the link to the full story.