

“SHE STOLE OUR COMPANY DATA – SHE HID IT IN HER UNDERWEAR!”

By Sharon D. Nelson, Esq. and John W. Simek © 2007 Sensei Enterprises, Inc.

She was your trusted personal assistant. She worked long hours, was good-natured, competent, reliable – a dream come true. Every day for the last several years, she came to work with her iPod, playing her favorite music softly through speakers on her desk. You never gave a second thought to that iPod.

Until the day she left. Perhaps your IT department alerted you to an unusual number of sensitive files being accessed. Perhaps you found out that your clients were being seduced away by a competitor for whom your assistant is now working. No matter how you found out, you are now experiencing the ultimate executive nightmare – a data heist.

iPods have storage memory – video iPods even have hard drives. We all see iPods every day and we all think of music. But iPods aren't just for music anymore. As computer forensics experts, we have now seen multiple cases where the innocuous seeming iPod was used to surreptitiously lift corporate data.

Mind you, the average data thief will simply slip the iPod in her purse or briefcase. But in this wacky, edgy world, there actually IS an iGroove panty for iPods (see the photo). Mind you, it is unlikely to be on my Christmas list or yours, but it provides yet another avenue for your data to escape.



The lesson here is simple for executives responsible for the protection of company data: you must take seriously each and every technological development which may compromise your security. Your IT department should be monitoring for unusual downloading and copying. You may not want to allow USB devices to be connected to devices on your network. If you do allow such connections, you may want them monitored. Perhaps access to all sensitive data should be logged.

Data thieves are notoriously clever – and management is constantly limping to catch up with technological advances. If it isn't the iPod carting off your data, it is the thumb drive, the smart phone, CDs and DVDs, web-based e-mails sent from local machines to avoid having them written to the server, etc. etc.

In a corporation of any significant size, it is imperative to do security reviews, at least annually, to try to stay ahead of both technology and the cleverness of miscreants. This is certainly an area where an ounce of prevention is worth a pound of cure. Once your data has been pilfered, damage control and legal remedies are both expensive and limited in what they can achieve. The damage to your company's reputation may be difficult if not impossible to retrieve – and the flood of data breach laws and data breach lawsuits has complicated an already maddening problem.

In a world where company secrets can depart a company via an employee's lingerie, constant vigilance is mandatory.

The authors are the President and Vice President of Sensei Enterprises, Inc., a computer forensics and legal technology firm based in Fairfax, VA. 703-359-0700 (phone)703-359-8434 (fax) sensei@senseient.com (e-mail), <http://www.senseient.com> (website)