Information Security – #1 Inventory your Assets

Overview
Understanding your information assets and access to information is essential to assessing security vulnerabilities. Whether you are an industry giant or a lean-and-mean one-person shop, you need to know your "information assets".

Step #1: Inventory your Assets
Here are some tips on conducting your own internal investigation to locate and classify your "information assets":

- *Inventory*. Inventory all servers, computers, flash drives, disks, and other equipment to find out where your company stores sensitive data. Also include laptops, employees' home offices, cell phones, and e-mail. No security audit is complete until you check everywhere sensitive data might be stored.
- *Interview*. Track personal information through your business by talking with your technology staff, human resources office, accounting personnel, and outside service providers. Get a complete picture of who sends your company sensitive data. Do you get it from customers? Call centers? Credit card companies? Banks or other financial institutions? What about affiliates and contractors?
- *Forms*. How does sensitive data come in to your company? Via your website? E-mail? Through the mailroom? What kind of information is collected at each entry point? Customers' credit card, debit, or checking account numbers? Do you receive sensitive health or financial data?
- *Access*. Who has, or could have, access to the information? Which of your employees has permission to look at or view sensitive data? Could anyone else get a hold of it? What about vendors who supply and update software you use to process credit card transactions? Do you have contractors that run your call center, distribution, or fulfillment operations?
- *Storage*. Different types of data present varying risks. Pay particular attention to how you store personally identifying information such as Social Security numbers, credit card numbers, checking account, or other financial information. Determine if the data you store can facilitate fraud or identity theft if it fell into the wrong hands.

Publication Information
Altius IT is a security audit, security consulting, and risk management firm. We are certified by the Information Systems Audit and Control Association (ISACA) as a Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Controls (CRISC), and Certified in the Governance of Enterprise Wide IT (CGEIT). For more information, please visit www.AltiusIT.com.