

Is Your Company ***AT RISK?***

How vulnerable is your business to corporate identity theft and the ensuing liability? Wondering how your company measures up when it comes to ID theft prevention? Take this test, and find out. For each item below, circle “**Y**” for yes or “**N**” for no.

1. Your human resources department conducts background checks before hiring all employees, particularly those who will have access to customers’ nonpublic information. **Y** or **N**
2. At each workstation and near each cash register there is a crosscut paper shredder for the disposal of “trash.”
Y or **N**
3. Personal information about employees and customers is kept in fireproof, secure file cabinets, and only designated employees can access this information with keys or, better yet, unique combinations assigned to each employee. **Y** or **N**
4. Instead of using Social Security numbers (SSNs) to identify employees and customers, your company uses alternate numbers. **Y** or **N**
5. Your company insists that its insurance providers use alternate numbers rather than their SSNs for employees’ insurance ID cards. **Y** or **N**
6. Your company has established security procedures for sending nonpublic information via fax, e-mail or telephone. **Y** or **N**
7. Your company requires all employees to wear badges including their photos for better identification and security. **Y** or **N**
8. Before disposing of computer discs, your company’s IT department permanently deletes all data and files.
Y or **N**
9. Your company stores personal information in restricted-access computer systems, so only a few qualified people can retrieve this data. **Y** or **N**
10. Employees are required to sign a Use of Confidential Information by Employee document, making employees aware of their legal responsibilities to protect your company’s nonpublic information. **Y** or **N**
11. Encryption and other IT safeguards have been installed for workplace computers, including laptops and PDAs, to secure the privacy of sensitive personal data. **Y** or **N**
12. Your company does not ask customers for information it does not need. Many companies do not need to know customers’ SSNs or driver’s license numbers to track and identify its customers. **Y** or **N**
13. Mandatory training is held regularly (typically yearly) for employees who have access to sensitive data. **Y** or **N**
14. Your company does not print employees’ SSNs in their entirety on paychecks (for both permanent and contract employees) or other identifying items such as parking permits, staff badges, time sheets, etc. **Y** or **N**
15. Your company has developed a written policy to protect nonpublic information and strictly prohibits the selling or sharing of employees’ and customers’ sensitive information. **Y** or **N**
16. Your company has written instructions on what it should do if nonpublic information is lost, stolen, or acquired electronically. **Y** or **N**
17. Your company has appointed an information security officer responsible for designing, implementing and monitoring a security program to protect the security, confidentiality and integrity of personal information about employee, customers and supplies. **Y** or **N**
18. Customers and employees are immediately notified if there is a computer security breach involving nonpublic information. **Y** or **N**

If you circled “**N**” even a few times, your company could be putting employees’ and customers’ sensitive data at risk. To learn more about how we can help protect your company, employees and customers, contact us for an appointment **TODAY!** This test is out of the *SMART SOLUTIONS* publication available from us.