



Expert Reference Series of IT Security White Papers

Preventing Identity Theft

www.thesolutionfirm.com

Check List: Preventing Identity Theft

Michael Gregg

Businesses are increasingly tasked with processing more and more amounts of electronic information. This can be especially burdening on small and medium-sized businesses because of their size and manpower. If they fail to handle this information properly, they may be just one click away from disaster. It's a valid possibility that the organization could be held liable if personal data is disclosed to an unauthorized person. The business could also suffer the loss of customers, revenue, and reputation.

Most organizations want to do the right thing and are interested in proper controls. Some may just feel overwhelmed by the day-to-day demands of business. A survey performed by *CIO magazine* found that 14% of respondents said their company had not taken any steps to protect customer information. If you are one of that 14%, take a look at these five basic steps to help start you off on a proactive footing for the New Year.

1. **Review state and local laws** - First examine any state or federal laws that your organization may be subject to and make sure you are compliant. Some states, such as California, have strict laws dictating businesses responsibilities while in possession of customer information. More than 450 privacy-related bills have been introduced in state legislatures in just the last several years.
2. **Create a privacy policy** - SMB's should develop policies that dictate what will be protected. These policies should detail what information is protected and be written in simple language that can be easily understood by customers.
3. **Implement technology to protect the information** – Make a solid effort to actually secure the information. Policies mean nothing unless organizations actually follow up and implement security controls. A commitment to data privacy means the organization has expended the funds necessary to adequately secure the data.
4. **Educate and train employees on the privacy policy** – Training is the life blood of any policy change. Don't expect employees to understand change unless they are informed and made aware of its importance.
5. **Publicly post the privacy policy** – The policy should be accessible by the organizations customers. Customers are the life blood of any business. They should know what steps the business is taking to protect their personal information including: name, address, credit card number, etc.

Customer data is a valuable corporate asset and as such deserves a sufficient level of protection. Customers expect that steps be taken to protect this information. In doing so, you are not only meeting expectations but also placing yourself ahead of the competition. If this is something that your organization has put off, now is the time to add this to your list of New Year's resolutions.

About the Author

Michael C. Gregg is the COO of Superior Solutions, Inc., a security assessment and training firm. His current responsibilities include performing security assessments and evaluations for corporate and government entities. He has served as the developer of high-level security classes, study guides, has taught classes for many Fortune 500 companies and contributed to many books, including the Syngress publication, *Hack the Stack*.

