

# Ten Fallacies about Identity Theft and Information Security

*Associations and their members may be dangerously unprepared.*

By: *Frank R. Mitchell, CITRMS*

*Tom Glanville, CITRMS*

According to the Privacy Rights Clearing House, approximately 350 million more records have been lost or stolen from businesses, schools, government agencies, and non-profit organizations since January 2005. Public pressure, as well as, increased scrutiny from regulators and legislators has produced new requirements, such as, the FACT Act Red Flags Rule, and Payment Card Industry Data Security Standards (PCI DSS). In light of these risks, why are associations and their members found to be dangerously unprepared?

Experts at Identity Theft Loss Prevention, LLC state that it is not concerns that organizations are aware of that put them at risk. This is a case of "what you don't know can hurt you." Here are TEN fallacies about identity theft and information security that NO ONE is talking about.

- 1. Identity theft is a consumer issue.** While individuals are ultimately the victims of identity theft, their information is often stolen from the organizations where they work or do business. According to the Privacy Rights Clearing House, over 341 million records have been lost or stolen from businesses, schools, government agencies, and non-profit organizations since January 2005! These information losses lead to damages for an organization including, state and federal fines, lawsuits, and a damaged reputation when individuals become victims of identity theft.
- 2. Our organization doesn't have "the kind" of information that thieves want.** Most organizations today only focus on protecting social security numbers and credit card information. However, today's identity thief can benefit from additional information including, but not limited to, birth dates, driver's license numbers, account numbers, and medical information. This information is vulnerable when collected, processed, transmitted, transported, stored, and disposed of for employees, customers, and vendors.
- 3. Our organization is too small.** When it comes to information loss size does not matter. In the case of an information security incident, the cost of federal and state fines, class action lawsuits, and a damaged reputation can be devastating to any size organization. According to the Disaster Recovery Journal, the U.S. Department of Labor has warned that 93% of businesses that experience a significant data loss go out of business within five years. "Of those companies 43% go out of business within the first year, and 72% go out in the second year."
- 4. I trust (or know) everyone that I do business with.** Trusting relationships with employees and customers is necessary for a successful enterprise. However, depending upon the study, 50% - 70% of information security incidents involve someone internally. The loss may be accidental or malicious. Proper policies, procedures, and training help to reduce these risks.
- 5. Information security is a technology issue.** Most organizations have taken some precautions to secure computers and networks. Just as important, stolen paperwork accounts for almost half (43%) of all identity theft (Javelin Strategy and Research, 2009). A comprehensive approach involving behaviors, operations, and technology is necessary to reduce risk and meet legal obligations.
- 6. I'm covered – we have an information security policy.** A policy document is where most organizations have begun and ended their efforts to reduce identity theft risk and to comply with the law. However, while a policy is a necessary evil, policy alone will not detect, prevent, or mitigate loss. Other requirements include designating an Identity Theft Prevention Officer (if you are a one man show, then it is you), risk assessment, training, plan for loss or breach, vendor oversight, implementation and governance.

7. **People's information is already available – I don't need to protect it.** Most states now have laws requiring the notification of those whose information was lost or stolen. In the event of a breach . . . 31% percent of your affected customers will terminate their relationship, 57% percent will lose trust and confidence in the company, 8% will file formal complaints (lawyers), 72% said there is a great chance they will become victims of Identity Theft (*Ponemon Institute Research Report, 2008*).
8. **It won't happen to me – show me an organization my size that has had a breach.** There are several websites that track information security breaches. The Privacy Rights Clearing House, [www.privacyrights.org](http://www.privacyrights.org), is a good resource. As you peruse the list of unfortunate organizations you may rationalize to yourself that they are too big, too small, wrong location, different industry, or different circumstances than your organization. Be careful! As long as any organization has information that is of value to a thief, there is a degree of risk.
9. **The government isn't enforcing these laws.** Both federal and state legislation is becoming more stringent for organizations of all sizes. As the economy struggles to recover and several new government initiatives need to be funded, the fines and penalties that can be generated from these laws can be substantial. Incidentally, if organizations are ultimately not held to task by lawmakers, then they should still take proper measures to protect information to mitigate loss from lawsuits and a damaged reputation.
10. **Protecting my organization from information security incidents is expensive.** Not taking PROPER measures to create an Identity Theft Prevention Program can be very expensive. There are firms that help small businesses, schools, government agencies, and non-profit organizations at affordable rates. A good comprehensive program includes education, risk assessment, policy, procedures, employee training, plan for loss or breach, resources, and continuing updates.

*Thomas Glanville and Frank R. Mitchell are Certified Identity Theft Risk Management Specialists with Identity Theft Loss Prevention, LLC. The company offers the field-tested and proven information Compliance and Awareness Process and ID Doctor to businesses, schools, government agencies and non-profit organizations. To find out how to protect your association and members visit [www.idtlp.com](http://www.idtlp.com).*