Identity Theft Resource Center:
Goldmine of Information

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Identity theft (IDT) continues to grow in the US and the world as electronic personally identifiable information (PII) about all of us increases in volume and dispersion. The Identity Theft Resource Center® (ITRC) provides excellent resources to help information assurance (IA) professionals and the public keep informed about current IDT developments and countermeasures.

ITRC is a non-profit organization sponsored by a wide range of organizations including commercial anti-IDT firms, grants from foundations, consumer-protection organizations, and law enforcement agencies.

The group’s mission statement is (quoting) to

- Provide best in class victim assistance at no charge to consumers throughout the United States.
- Educate consumers, corporations, government agencies and other organizations on best practices for fraud and identity theft detection, reduction and mitigation.
- Provide enterprise consulting and outsourced services related to information breach, fraud and identity theft.

Their philosophy is summarized on their Web site as follows:

- The ITRC fundamentally believes that both consumers and businesses are victims of identity theft and fraud.
- Prevention and reduction of identity theft will require education and cooperation between consumers, businesses, law enforcement agencies, and legislators.
- The ITRC believes that support and education of businesses has a strong positive impact on the restoration of victims’ lives, and the prevention of further identity theft.
- The ITRC has consciously avoided legal advocacy as a method of forwarding its mission.

I asked Linda Foley, the Founder and Chairman of the ITRC, to explain this last point. She explained, “ITRC believes that it is critical that we work as a team whenever we can: law enforcement, business, government, consumers and advocates. We have found that once a problem has been addressed with the correct person at a company, litigation is not needed. ITRC maintains a centrist position and, as such, has found that entities are open to discussing matters with us to resolve common issues.”

The ITRC keeps a record of publicly disclosed data breaches; this list is updated daily and published every Tuesday. “To qualify, breaches must include personal
identifying information that could lead to identity theft, especially the loss of Social Security numbers. ITRC follows U.S. Federal guidelines about what combination of personal information comprise a unique individual, and the exposure of which will constitute a data breach.”

“There are currently two ITRC breach reports which are updated and posted on-line on a weekly basis.

- The ITRC Breach Report presents individual information about data exposure events and running totals for a specific year.
- The ITRC Breach Stats Report develops some statistics based upon the type of entity involved in the data exposure. Breaches are broken down into five categories, as follows: business, financial/credit, educational, governmental/military and health care. Other more detailed reports are generated throughout the year and posted on a quarterly basis.”

When I checked the breach reports in early July 2009, there were 268 breaches analyzed covering a total of over 12M records. The database includes these fields:

- ITRC Breach ID
- Company or Agency
- State
- Estimated Date
- Breach Type (e.g., electronic, paper data)
- Breach Category (e.g., Educational, Government/Military, Banking/Credit/Financial)
- Records Exposed?
- # Records Reported
- Attributions (publication data such as source, date, author, title, URL)

This database is an invaluable research resource for everyone interested in studying the issue of IDT.

In addition to these scholarly reports, the Web site also includes:


Finally, the ITRC offers a US toll-free number for victim assistance: 800-400-5530.

I recommend that readers include information about this organization in their security awareness materials for employees, students and their families.

* * *

In part 2 of this two-part sequence, I’ll summarize highlights from the valuable report entitled, “Identity Theft: The Aftermath 2008.”

* * *
Join me online for three courses in October and November 2009 under the auspices of Security University. We will be meeting via conference call on Saturdays and Sundays for six hours each day and then for three hours in the evenings of Mon-Tue-Wed-Thu. The courses are “Introduction to IA for Non-Technical Managers,” <http://www.securityuniversity.net/classes_online_Intro_Info_Assurance.php> “Management of IA,” <http://www.securityuniversity.net/classes_online_Mgmt_Info_Assurance.php> and “Cyberlaw for IA Professionals.” <http://www.securityuniversity.net/classes_online_Cyberlaw_IA_Professionals.php> Each course will have the lectures and discussions recorded and available for download – and there will be a dedicated discussion group online for participants to discuss points and questions. See you online!

* * *

M. E. Kabay, PhD, CISSP-ISSMP <mailto:mekabay@gmail.com> specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/> 

Copyright © 2009 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.