

Preventing Identity Theft Throughout the Data Life Cycle

by Marilyn Prosch

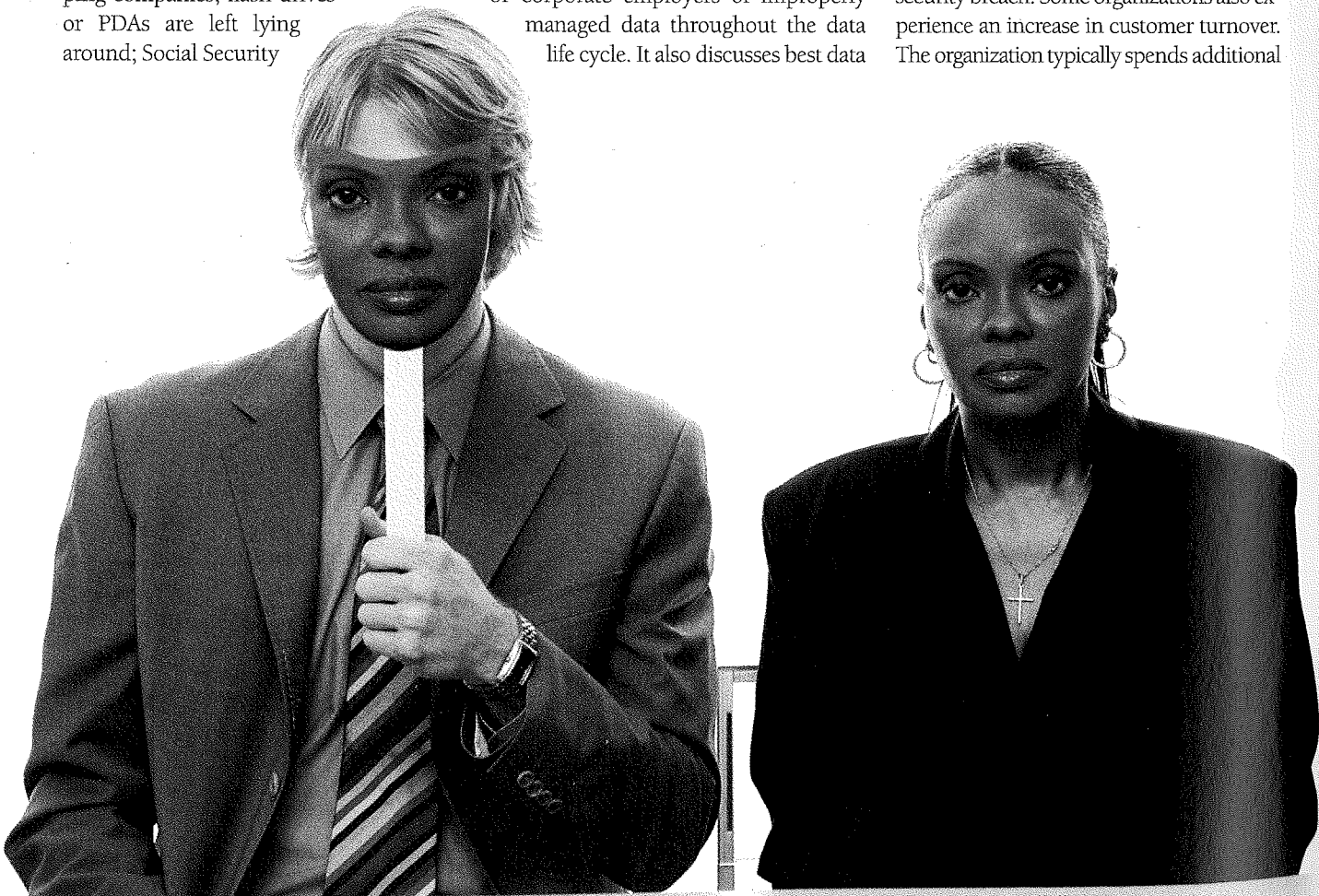
The Federal Trade Commission estimates that as many as 9 million people have their identities stolen every year. According to the Privacy Rights Clearinghouse, more than 200 million instances of data breaches have occurred since the beginning of 2005, and they show no signs of letting up. In the first quarter of 2008 alone, more than 85 million incidents were reported.

The causes of data breaches run the gamut: Hackers get unencrypted, transmitted data and data at rest; laptops are stolen or lost; storage devices are lost by third-party shipping companies; flash drives or PDAs are left lying around; Social Security

numbers are accidentally printed on envelopes; or data is found on discarded computers. This article examines the organizational risks to CPAs and their clients or corporate employers of improperly managed data throughout the data life cycle. It also discusses best data

management practices and proper procedures for responding to a data breach.

Data breaches, whatever the cause, are costly. According to a study by the Ponemon Institute, the average cost of a data breach in 2007 was \$6.3 million. The average cost to an organization per record compromised is about \$197, which is typically spent on phone calls for customer notification, providing free credit monitoring, discounts on membership fees, or discounts on merchandise to make up for the security breach. Some organizations also experience an increase in customer turnover. The organization typically spends additional



money in data. Companies should also have the policies that must be put in place for the next 10 years.

DATA LIFE CYCLE MANAGEMENT

Data life cycle management covers all of the processes that control the flow of data throughout its creation to when it is no longer required or is required to be deleted. Data may be lost or stolen in many cases, such as by identity thieves. If sensitive information is lost, the numbers, the time. Organizations should work with the late PI with the late enhancing technology. The number and current need to diligence of age and state.

As data security increases, many

OR

believe little control. They should regularly purge sensitive information. Identity theft is no longer a niche issue. It is a major cause for concern. The purpose of an audit or other review of the organization's data is to ensure that, where possible, possession

- CPAs and corporate employers should focus on privacy by educating customers about identity theft.
- Data may be a major organizational value to identity theft. Data containing personally identifiable information (PI), such as

money in data protection enhancements. Companies sanctioned by the FTC may also have the added cost of security audits that must be performed every two years for the next 10 to 20 years.

DATA LIFE CYCLE MANAGEMENT

Data life cycle management (DLM) includes all of the processes involved in managing the flow of data throughout its life cycle: from creation to when it has lost its business value or is required by law to be deleted. Although data may lose its value to an organization, in many cases, it does *not* lose value to identity thieves. If aging data contains personal information (PI), such as Social Security numbers, the value does not diminish over time. Organizations that protect only newer PI with the latest encryption and privacy enhancing technologies are placing their former and current customers at risk. They need to diligently protect all PI, regardless of age and storage medium.

As data storage costs continue to decrease, many organizations mistakenly be-

tential liability.

PI typically flows through the following life cycle phases: collection and transmission; storage; processing and use; sharing/replication; and destruction. Throughout this process, PI may be transmitted electronically from a personal computing device to server to third party and back. Each phase is examined below, and the risks of gaining access to the PI are discussed as well as privacy mitigating strategies.

DATA COLLECTION AND TRANSMISSION

Identity theft concerns are focused on the security and necessity of the collection process. Collecting PI just because you can is unsafe. Organizations can reduce privacy risks by *not* collecting unnecessary PI. Once PI gets into the data life cycle pipeline, the cost of managing and destroying it escalates.

PI may be obtained through many mechanisms and technologies. For example, paper-based forms, such as credit card

it should be destroyed immediately afterward since the PI is now recorded in the organization's database. Tax accountants face similar challenges with tax receipts and documents clients bring to their office. The destruction section below highlights good paper-based PI destruction methods.

For PI that is initially collected electronically, the organization must provide appropriate security. Strong encryption of data as it is being transmitted is required, regardless of whether the PI is collected from a wireless network inside an organization or via the public Internet. The strength of an encryption application is generally a function of the strength of its underlying algorithm and the length of the encryption key. Assume the data can be intercepted, and encrypt it. Authentication may be necessary during collection, depending on the type and sensitivity of PI. Challenge questions, biometric devices and one-time passwords are low-cost solutions. Biometric readers and one-time password devices can both be implemented for less than \$100 per user once the server management software is installed.

DATA STORAGE

After data is collected and transferred to its storage location, it must be protected from unauthorized access by both internal and external sources to prevent identify theft. Regarding internal sources, PI needs to be clearly identified by management and necessary controls designed and implemented to protect it from unauthorized internal access. Identity theft rings have been known to recruit internal

Although data may lose its value to an organization, in many cases, it does *not* lose value to identity thieves.

lieve little cost incentive exists to periodically purge old PI. However, from an identity theft prevention perspective, if the PI is no longer relevant for the original purpose for which it was stored or is not part of audit or other regulatory requirements, the organization should purge it. Otherwise, possession of unnecessary PI is a po-

applications completed at booths in public locations, such as airports and sporting events, need to be protected. Forms should be immediately transferred to a secure place, where they cannot be lifted or viewed by another individual visiting the booth. If a paper-based document is manually keyed or scanned into a computer,

EXECUTIVE SUMMARY

■ **CPAs and their clients or corporate employers** are susceptible to privacy breaches, leaving their customers and employees at risk of identity theft.

■ **Data may lose its value to an organization, but it may not lose value to identity thieves.** If aging data contains personal information (PI), such as Social Security num-

bers, the value does not diminish over time. Organizations that protect only newer PI are placing their former and current customers at risk.

■ **Personal information is at risk during all phases** of the data life cycle, and the possession of unnecessary personal information is a potential liability.

■ **Although the risk of a privacy breach can be reduced, it cannot be eliminated.** Companies and CPA firms that collect, use or store PI should have well-planned and documented response strategies. When a breach occurs, an organization needs to act quickly.

■ **Knowledgeable CPAs can leverage the principles and cri-**

teria in the AICPA's Generally Accepted Privacy Principles (GAPP) to help reduce the negative consequences of data breaches.

Marilyn Prosch, Ph.D., CIPP, is a professor at Arizona State University and a member of the AICPA Privacy Task Force. Her e-mail address is marilyn.prosch@asu.edu.

FACTA Identity Theft "Red Flags"

What are they? The Federal Trade Commission and the federal financial institution regulatory agencies have issued rules on identity theft "red flags" and address discrepancies. The final rules implement sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003.

Who made these rules? They were issued by the Board of Governors of the Federal Reserve System, the FDIC, the Federal Trade Commission, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision.

When are they effective? Final rules became effective Jan. 1, 2008. Most of the agencies required covered financial institutions and creditors to comply by Nov. 1, 2008. The FTC extended its effective date until May 1, 2009.

What do they require? Each financial institution and creditor that holds any consumer account, or other account for which there is a reasonably foreseeable risk of identity theft, must develop and implement an Identity Theft Prevention Program for combating identity theft in connection with new and existing accounts.

The program must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft and enable a financial institution or creditor to:

1. Identify relevant patterns, practices, and specific forms of activity that are red flags, signaling possible identity theft, and incorporate those red flags into the program;
2. Detect red flags that have been incorporated into the program;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
4. Ensure the program is updated periodically to reflect changes in risks from identity theft.

Source: www.ftc.gov/opa/2007/10/redflag.shtm.

employees. Paper-based filing systems should be protected with locks. If feasible, a file librarian should have custody of the files and keep a log of checkouts.

Protection of digitally stored data should take two lines of defense: preventive and detective. Preventive techniques include: (1) placing properly configured and well-maintained firewalls around the PI to prevent external hackers from gaining access; (2) using strong authentication techniques for authorized internal users; and (3) strongly encrypting PI to render it useless if lost or stolen. This latter technique is especially important if the PI is stored on a laptop. For example, most life insurance salespeople input customers' PI into their laptops and periodically transmit it to headquarters. The PI should be strongly encrypted so that if the laptop is lost or stolen, it will not be compromised. The use of encryption for PI residing on all storage mediums, including flash drives, CD/DVDs, PDAs, and radio frequency identification (RFID) devices, is critical to minimizing the risk of identity thieves gaining access to it.

DATA PROCESSING AND USE

While PI is processed and used, it must be protected. A primary concern is that PI will be erroneously processed and accidentally exposed. Last year, 5,000 taxpayers in Wisconsin had their Social Security numbers exposed in a state mailing. The cause

assistant professor at Harvard University posted steps online for viewing customer purchase data on a large department store's Web site (www.benedelman.org/news/010408-1.html). Within days of this posting, a \$5 million class action suit was filed against the online division of the retailer.

Unfortunately, unintentional processing errors have plagued organizations since the early days of computerized systems; however, organizations must strive to improve their processes and controls to protect PI. Damage control is costly, and the court of public opinion harsh. If an error does occur, a good incident response plan is crucial.

DATA SHARING AND REPLICATION

Technological advances make data replication increasingly cheaper and easier to accomplish. Protecting replicated data presents a challenge. When PI is involved, training and policies should be in place to guide employees, such as logging downloads of PI. Software is available to periodically scan personal computing devices and storage mediums to "intelligently" look for different types of stored PI.

Once an organization collects PI, it may be forwarded to other business units, companies, or third parties for a variety of reasons, such as to complete a transaction, share marketing data, or comply with reg-

The use of encryption for PI residing on all storage mediums is critical to minimizing the risk of identity thieves gaining access to it.

was a simple processing snafu: A faulty machine incorrectly folded the mailings, allowing the numbers to be seen through the clear address window of the envelope. If PI must be printed and sent through the mail, the outputs of the process need to be routinely inspected to ensure that human or machine error is not allowing the information to be exposed.

Electronic data processing can also result in the exposure of PI. Last year, to demonstrate company security lapses, an

ulatory requirements. Keeping a log of the locations where each copy resides can seem insurmountable. However, if the "data trail" is not tracked and well-protected, an organization can place its customers at risk of identity theft and be plagued by bad press.

Another large retailer's name was thrust into the news earlier this year when the data storage company of a third-party information processor announced that a computer storage tape was "missing." The

best possible would have strongly encrypted and its unable to pro organizations that third party ing stored PI.

Organizations copies of PI need to be aware will handle The third practices mu allow the se tion to comp cy commitm notice, and t tion needs t garding this. this is to rec of the contro ice provider.

A SAS 70 lows a servic control poli uated and party. Howe ment only o financial re not include the AICPA practitioner uation. Alth evant, the A working to tion guidar (This guida ument Effe Provider in Engagement, ITJOA.)

The red practice to CPAs may l tax returns instances w should be riodic review a remarried minimum, children's moved bel

best possible response to this type of news would have been that the lost PI was strongly encrypted. Unfortunately, the retailer and its third-party processor were unable to provide such assurances. Organizations that outsource need to ensure that third parties are adequately protecting stored PI.

Organizations that forward or send copies of PI to a third party need to be aware of how they will handle and protect it. The third party's privacy practices must be sufficient to allow the sending organization to comply with its privacy commitments in its privacy notice, and the sending organization needs to obtain assurances regarding this. One way to accomplish this is to request a third-party audit of the controls at the third-party service provider.

A SAS 70 Type II engagement allows a service organization to have its control policies and procedures evaluated and tested by an independent party. However, since a SAS 70 engagement only covers internal controls over financial reporting, which typically do not include controls related to privacy, the AICPA issued guidance in 2001 to practitioners addressing this type of situation. Although this guidance is still relevant, the AICPA Privacy Task Force is working to update its service-organization guidance with a focus on privacy. (This guidance can be found in the document *Effects of a Third-Party Service Provider in a WebTrust SM/TM or Similar Engagement*, available at www.aicpa.org/ITJOA.)

The redaction of PI is another good practice to help prevent identity theft. CPAs may be asked to provide copies of tax returns for their clients in a variety of instances where Social Security numbers should be removed. For example, in periodic reviews of child support payments, a remarried taxpayer should have, at a minimum, a new spouse's and any stepchildren's Social Security numbers removed before the tax documents are

handed over to the ex-spouse. Once all PI is removed from copies, only the original document needs to be protected from identity thieves.

DATA DESTRUCTION

The final and critical phase in the data life cycle is the appropriate destruction of PI, both paper-based and electronic. CPAs and their clients want to avoid having a state attorney general file a claim against them as did Texas' attorney general against a physical therapy company that exposed more than 4,000 pieces of its customers' records, including Social Security numbers, by placing them in garbage containers behind a building. The method of destruction depends on the type and sensitivity of the PI. As mentioned earlier, the business value of PI typically declines over time, and, ultimately, it can become a liability.

Consider that last year the fence of a school district warehouse in Pennsylvania was littered with letters containing the names of district employees, along with their bank account numbers and Social Security numbers. The forms were more than

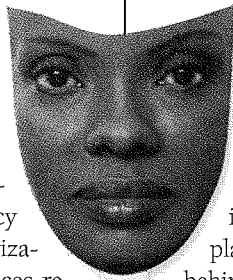
10 years old, but they still contained PI that is just as valuable today to identity thieves. Data destruction techniques vary widely in type and cost. CPAs can provide valuable advice to their clients about best practices for destroying PI.

RESPONDING TO A PRIVACY BREACH

The risk of a privacy breach can certainly be lowered by implementing some of the techniques mentioned in this article, but the risk cannot be eliminated. Human error will occur, and hackers will continue to break into systems. Good privacy practices and procedures should significantly reduce the risk, while demonstrating an organization's commitment to privacy protection.

Companies and CPA firms that collect, use or store PI should have well-planned and documented response strategies. When a breach occurs, an organization needs to act quickly and smartly. A 2008 research study I completed with Vernon Richardson, the Accounting Department chairman at the University of Arkansas, found that the longer a company waits to report a breach, the more its stock value drops when the event is finally reported. An organization does not want the public to think it tried to cover up the breach or put individuals at increased risk by delaying notification.

Have a plan and form a team. The AICPA, along with the Canadian Institute of Chartered Accountants (CICA), developed an Incident Response Plan for privacy breaches. This document arms organizations with a well-defined, organized approach for handling breaches, as well as identifying appropriate actions to take when the source of the intrusion or incident at a third party is traced back to the organization. The plan identifies and describes the roles and responsibilities of the Incident Response Team, the group responsible for putting the plan into action. The team needs to be well-trained and ready for immediate action. No organization needs a rookie handling a privacy breach. The team should be



Data Eradication

Typical methods of destruction include:

- Render storage device unusable.
- Burn data or storage device.
- Pulverize storage device.
- Shred data.
- Overwrite/delete/wipe clean storage device.

Issues to consider when contracting with a third-party destruction vendor:

- Verify the third-party vendor has certification, such as NAID.
- Identify key items to include in a service-level agreement, including:
 - ▶ Responsibilities of the service provider.
 - ▶ How and when destruction will occur and by whom.
 - ▶ Certificate of destruction.
 - ▶ Ability to visit facility and witness destruction.

authorized to take appropriate steps to contain, mitigate or resolve a computer security incident.

Data breach notification. If an organization has PI that has been breached, it should notify the respective individuals as quickly as possible. When confirmation of a privacy breach has occurred:

- Notify the Incident Response Team.
- Coordinate with the chief privacy officer and legal counsel on the timing, content and method of notification.
- Prepare and issue a press release or statement, if needed or desired.

The press will find out about the breach if individuals are notified. Therefore, the best defense is to be proactive and inform the public, emphasizing that the breached organization values good data protection and has acted in good faith. This is a good opportunity to emphasize the privacy-enhancing policies and procedures in which the breached organization has invested. Have all of this information available to the Incident Response Team *before* a breach occurs.

CONCLUSION

An organization faces many PI protection challenges in today's business environment

and technological world. Ontario Privacy Commissioner Ann Cavoukian often says that, "Potential conflicts between business demands for personal data and individuals' privacy may be reconciled through smart planning, good management and controls, and the use of privacy-enhancing technologies, resulting in a 'win-win' positive-sum solution. Good privacy is good business."

Developing protection strategies throughout the data life cycle is one such

method organizations can use to move their data protection strategies along the privacy maturity curve. A comprehensive set of privacy principles, Generally Accepted Privacy Principles (GAPP), has been developed by the AICPA/CICA to provide detailed guidance for CPAs and their clients/organizations for the issues discussed in this article. ❖

AICPA RESOURCES

Articles

- "The Human Element: The Weakest Link in Information Security," *JofA*, Nov. 07, page 44
- "Help Prevent Identity Theft," *JofA*, June 07, page 30
- "Phight Phraud," *JofA*, Feb. 06, page 43
- "The Small CPA Firm and Privacy Services," *The Practicing CPA*, Sept. 06, www.aicpa.org/Magazines+and+Newsletters/Newsletters/The+Practicing+CPA/September+2006/small.htm

IT Center and CITP credential

The Information Technology (IT) Center provides a venue for CPAs, their clients, employers and customers to research, monitor, assess, educate and communicate the impact of technology developments on business solutions. Visit the IT Center at www.aicpa.org/INFOTECH. Members who want to maximize information technology to increase efficiency and boost profits may be interested in joining the IT Member Section or pursuing the Certified Information Technology Professional (CITP) credential. For more information about the IT Member Section or the CITP credential, visit www.aicpa.org/IToffers. For privacy standards, rules and regulations, visit the IT Center's Privacy/Data Protection page at www.aicpa.org/privacy.

OTHER RESOURCES

Web sites

- *Secure Destruction of Personal Information*. This fact sheet recommends best practices for the secure destruction of records containing personal information. It is available at www.ipc.on.ca/index.asp?navid=46&fid1=451.
- The National Association of Information Destruction (NAID) promotes the information destruction industry and the standards and ethics of its member companies. The NAID can be found online at www.naidonline.org.

Generally Accepted Privacy Principles

The AICPA and the Canadian Institute of Chartered Accountants (CICA) formed the AICPA/CICA Privacy Task Force, which developed the Generally Accepted Privacy Principles (GAPP). Using GAPP, CPAs can help organizations design and implement sound privacy practices and policies. Businesses that implement privacy policies in accordance with GAPP will likely meet, if not exceed, most applicable privacy laws and regulations while reducing privacy-related risks. GAPP can be downloaded free at www.aicpa.org/privacy.

Also, many checklists and brochures on using GAPP in practice can be downloaded from the above site, including, but not limited to:

- **Incident Response Plan.** The Incident Response Plan template can be used to help design, develop or adapt a plan and better prepare for the handling of a breach of PI.
- **Privacy Checklist for CPA Firms.** This checklist gives CPA firms a practical illustration of selected portions of GAPP to maintain privacy best practices within organizations.
- **Privacy Services Prospect Checklist.** This checklist helps practitioners in small and medium firms focus their marketing efforts by identifying characteristics of existing and prospective clients that will experience the greatest benefit by investing in privacy services.

CPA Firm Data Breaches

December 2007: A laptop containing the PI of an undisclosed number of partners, principals and other employees of a large accounting firm was stolen while in possession of a contractor responsible for scanning the accounting firm's pension fund documents.

April 2007: The headquarters of a large public school system had two laptops stolen that belonged to its accounting firm and its subcontractor. They were reviewing contributions to the teachers' pension fund. The PI of 40,000 individuals was compromised.

June 2006: An unencrypted laptop belonging to an online travel group's auditor was stolen. It contained information on potentially 250,000 individuals.

The C
LI

As a
leav
integral
One of
take to
your de
finding
you need
daunting

Afford
Coverag
Plan, is
Compar
benefits
of finan
And wit
to search
your lif
you wan

Eligible
\$2 mill
your lo
living e
a child
approve
the age
Select S
standar

Option
You ma
optiona
provide

The Pruden
Guam, Pue
751 Broad
Series 313
is a Divisio
IFS A1139