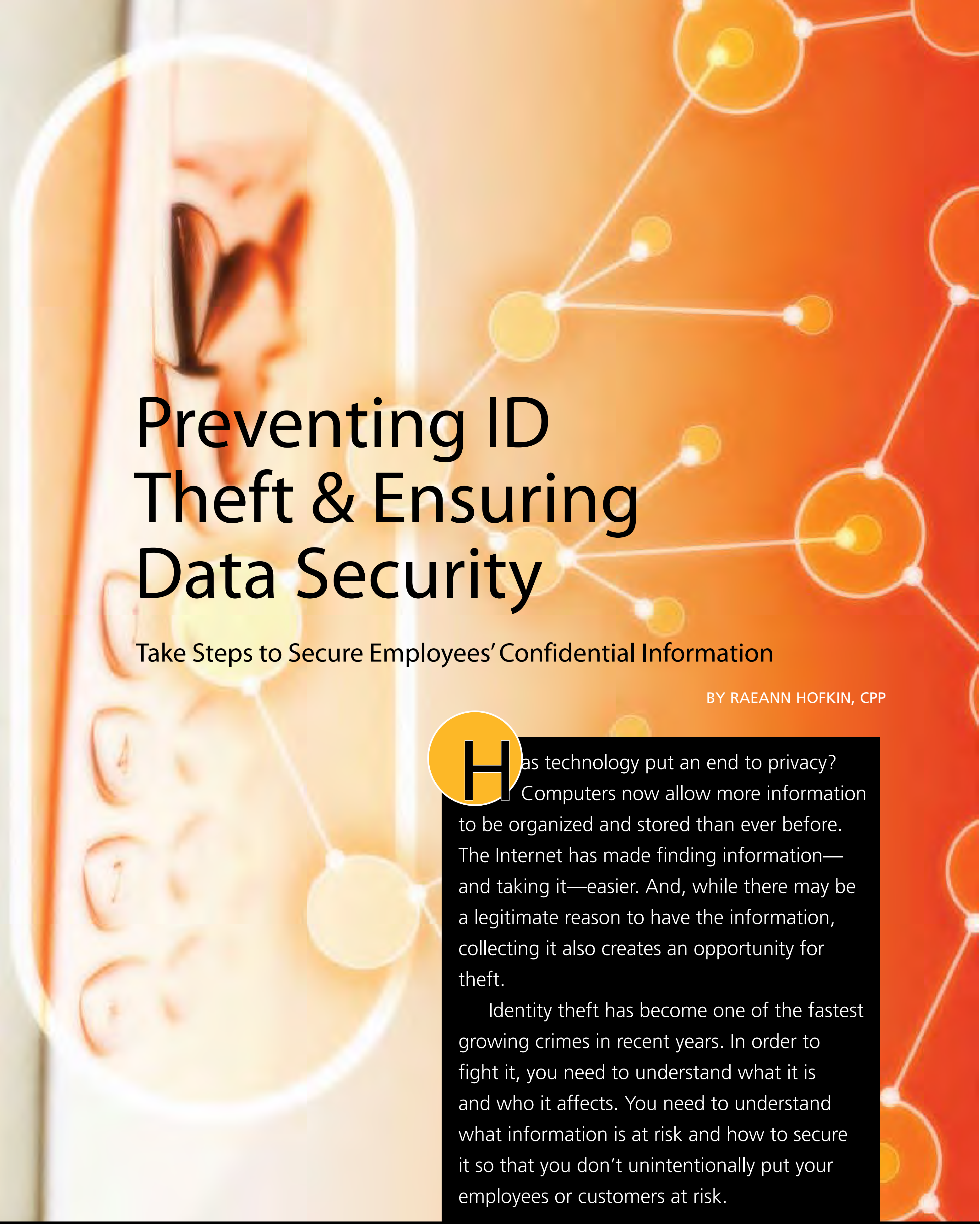

Preventing ID Theft & Ensuring Data Security

Take Steps to Secure Employees' Confidential Information

BY RAEANN HOFKIN, CPP

Has technology put an end to privacy? Computers now allow more information to be organized and stored than ever before. The Internet has made finding information—and taking it—easier. And, while there may be a legitimate reason to have the information, collecting it also creates an opportunity for theft.

Identity theft has become one of the fastest growing crimes in recent years. In order to fight it, you need to understand what it is and who it affects. You need to understand what information is at risk and how to secure it so that you don't unintentionally put your employees or customers at risk.

The Problem

Currently, there aren't any legal mandates regarding how to develop, maintain, and enforce an information security program. In fact, current law fails to stipulate what constitutes an "information security program" or publish any legal standards for security.

Legislation continues to be enacted to deal with the crime of identity theft, but legislation alone will not prevent it. Most current laws are neither proactive nor preventative.

In addition, the legislative process takes too long to address the problems. By the time a law is enacted, the ID thieves have already found a better way around the "speed bump." In a nutshell:

- The laws are reactive and hastily enacted after lengthy political wrangling.
- Many legislators lack knowledge about the crime, criminal, and the victim.
- If there is a punishment, it fails to deter the criminal.
- You often can't even be convicted of identity theft unless you are involved in some other criminal activity as well.

Organized criminal groups don't waste time breaking into our personal mailboxes—they want the large corporate databases. According to recent articles in the IAPP newsletter, more and more identity thefts are committed inside the workplace by a dishonest few employees who steal the social security numbers (SSNs), credit cards, banking, or other personal information from their coworkers or customers.

Don't let your company be an easy target. Computer security alone will not work, because computers don't steal identities—people do! You need to secure the people and the processes, not just the IT property.

Your Responsibility

As payroll and HR professionals, you are in a unique position to help secure your company's data. Be proactive and aware of the potential for workplace theft. With diligence, you can implement changes to prevent ID theft from happening at your company.

As a payroll professional, you are closest to the workplaces and work processes where identity thefts can occur. You perform the tasks required to process, update, maintain, and manage personal information on applications, healthcare forms, payroll, and benefits—both paper and digital.

As a payroll professional, you will be able to recognize the work processes most susceptible to identity theft. Therefore you are also the key to securing that sensitive data.

Each department that plays a role in a particular process should play a role in analyzing the process and eventually securing it. Focus on the job positions, not the employee. People come and go, but the position remains stable.

Identity theft is here to stay because it is a low-risk offense with high payoffs. It is relatively easy to access SSNs because they are so widely used. Most every business today has at least one database with SSNs for all employees. Every business has a payroll system containing all the information needed to steal identities.

According to the FTC, it's been estimated that at least 14% of the ID thefts in the United States are perpetrated from within companies. The insider who steals identities may be a part-time, full-time, temporary, or permanent employee. He or she may even be an impersonator specifically hired into the company to steal identities.

A Plan of Defense

Develop a plan to secure your company's data. At the very least, do your part to secure your employees' confidential information. Start changing your company culture to make privacy a top priority. This can

Quick Picks & Short-Term Fixes

- Practice vigilance and learn from your mistakes.
- Put policies in place so you don't repeat mistakes.
- Enforce your written policies with surprise audits.
- Develop and enforce a "clean desk policy."
- Managers should walk around in the evening and cite people who do not have confidential information secure (anything on the fax? In the open? Are all the drawers locked?).
- Use "out of office" cards. Employees put them on their desk when they are out of the office so nobody leaves confidential information.
- What was changed, who changed it, and did that person have access and authority? You may already be doing this as a SOX requirement.
- Lock your computer when you walk away by clicking "CTRL, ALT, Delete" and click on the "lock computer" button.
- Password protect your screen saver—make this a company policy.
- Move printer and fax to inner office (or pull the paper out when you leave for the night).
- Retrieve faxes when received.
- Wait at fax until document has been sent.
- Do not leave originals in fax machine or copier.
- Lock file cabinets at all times.
- Think about what you are throwing away—should it be shredded? Where is the shredder? Do people know?
- Any paperwork with personal information that is not needed should be shredded at the end of the day.
- Make sure documents are shredded before walking away from shredder.
- Do not leave identifying information on voicemail messages or e-mails.
- Evaluate performance on all privacy procedures (add it to the employees' goals and objective EVERY year).
- Don't store sensitive information on your laptop hard drive.
- Hand deliver confidential information.
- Keep personnel and payroll files in locked area with restricted access.
- Use firewall and antivirus software.
- Reduce spam and phishing with filters, then update the filters as necessary.
- Audit your companies' laptops. Do you know who has what laptop? Are they all "accounted for?

Be Proactive!

Sign up to receive a free newsletter on data privacy by visiting www.privacyassociation.org.

be slow and painful, but the challenge is too important to leave to someone else. Take the lead today!

Start by creating a project team. Elect, select, or seek volunteers who will investigate and make recommendations to upper management and will audit for security. Form a project team that will develop standards to secure business information processes and the company's virtual property. It's a good idea to involve someone from IT, HR, finance, and payroll. Don't discount people because they are too busy—they are the ones who get things done.

After you select your key people, put the call out for more volunteers. With a project like this, the more people you will have involved, the more ideas that will be generated and the more hands you have will to push through the recommended changes. Also, you should open up the project to new members every now and then. A new perspective and fresh ideas will add value to the team.

Employees with job experience may produce ideas that would add value to the new security orientation program. Employees involved in the process tend to take responsibility for the outcomes. Keep in mind, employees who feel they contributed to the program tend to promote and perpetuate the practices or policies they propose.

For this reason, it is important to include as many employees as possible in the company initiative. Ask for written anonymous comments and suggestions to improve the program. Then make feasible changes.

Once you have your project team in place, work on securing your people. Businesses set the standards of integrity and performance for their own workforce, *intentionally or not.*

Beginning with recruitment, the company can purposefully use scientific procedures to assemble a capable group of workers. Or they can leave things to chance. Personnel tests can be used to select job applicants for performance, motivation, and integrity. Perform background checks on ALL employees including part-time, full-time, temporary workers, third-party vendors, and any positions that may be outsourced (e.g., cleaning service). If this is not feasible in your organization, it should at least be done for employees with access to sensitive information and the areas where it is kept.

Putting the Plan Into Action

Now you are ready to work on securing the processes. Identify both internal and external job positions that require knowledge of confidential information. Know the types of personal and business information used in departmental job tasks, such as credit cards, bank accounts, SSNs, passwords, and computer systems.

Trace the flow of information as it is processed through the department, by tracing the flow of the documents that contain such information. Determine the locations in the process where the information is most susceptible to theft.

Secure the information process across departments. Be certain to distinguish between how the information is processed and where it is processed. ID theft can occur during distribution, delivery, and sorting of documents or by taking them from a desk, mailbox, or computer. How is information distributed, delivered, or sorted? Where is it distributed—to a desk, or mailbox, or computer?

In other words, follow the document (containing the identity) from its source through the job position that performs the standard job task. A job title may suggest the job is a position with an impact on security, but job titles do not fully describe jobs. Be sure to focus attention on the job process, not the person who holds the job. It is the job process that needs to be secured. Remember, people come and go, but the job remains stable.

Create a timeframe to implement changes. What are your quick picks—those that can be done immediately at no cost? What are your short-term goals that can be implemented with little effort and low cost? What are your long-term goals that will require budgeting and formal approval from upper management? Be realistic and specific with target dates.

Buying a piece of software will not fix the problem. Just like spam, phishing, and viruses, ID theft will be around for years to come, perhaps forever. But it's also a call to action for businesses that want to safeguard their sensitive information and that of their employees and customers.

Raising awareness, especially among those with access to personal information, will create an environment where employees are easily alerted to suspicious activity. An environment of awareness, privacy policies, and proper oversight and controls will protect the most sensitive employee and customer information. This could deter an ill-meaning party from assuming your identity and doing your employees harm.

Raeann Hofkin, CPP, is Payroll and Accounts Payable Manager for Telerx Marketing and the Southeastern Pennsylvania Chapter President.