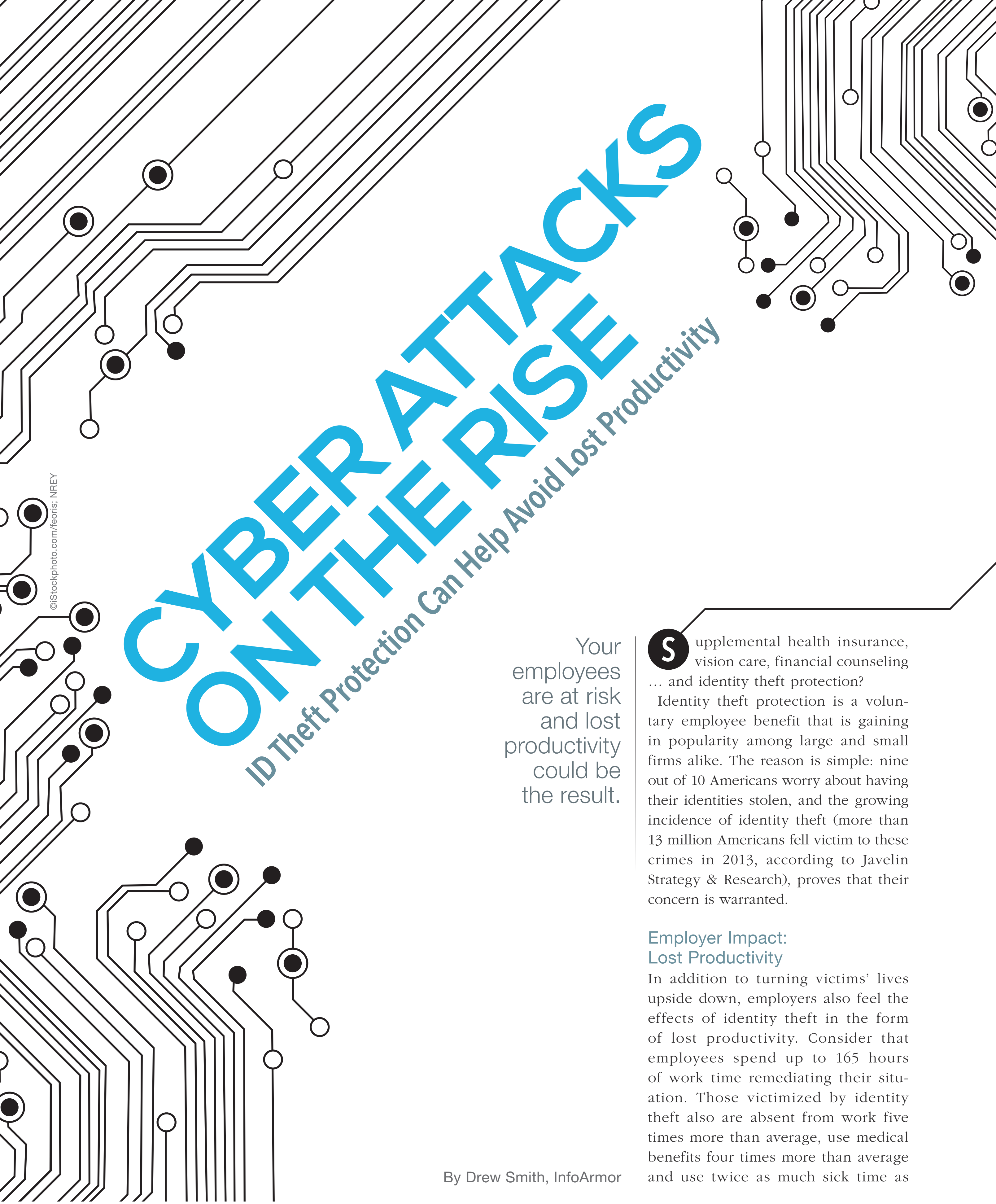
workspan

The Magazine of WorldatWork©

04 | 2015



©iStockphoto.com/feoris; NREY

CYBERATTACKS ON THE RISE

ID Theft Protection Can Help Avoid Lost Productivity

Your employees are at risk and lost productivity could be the result.

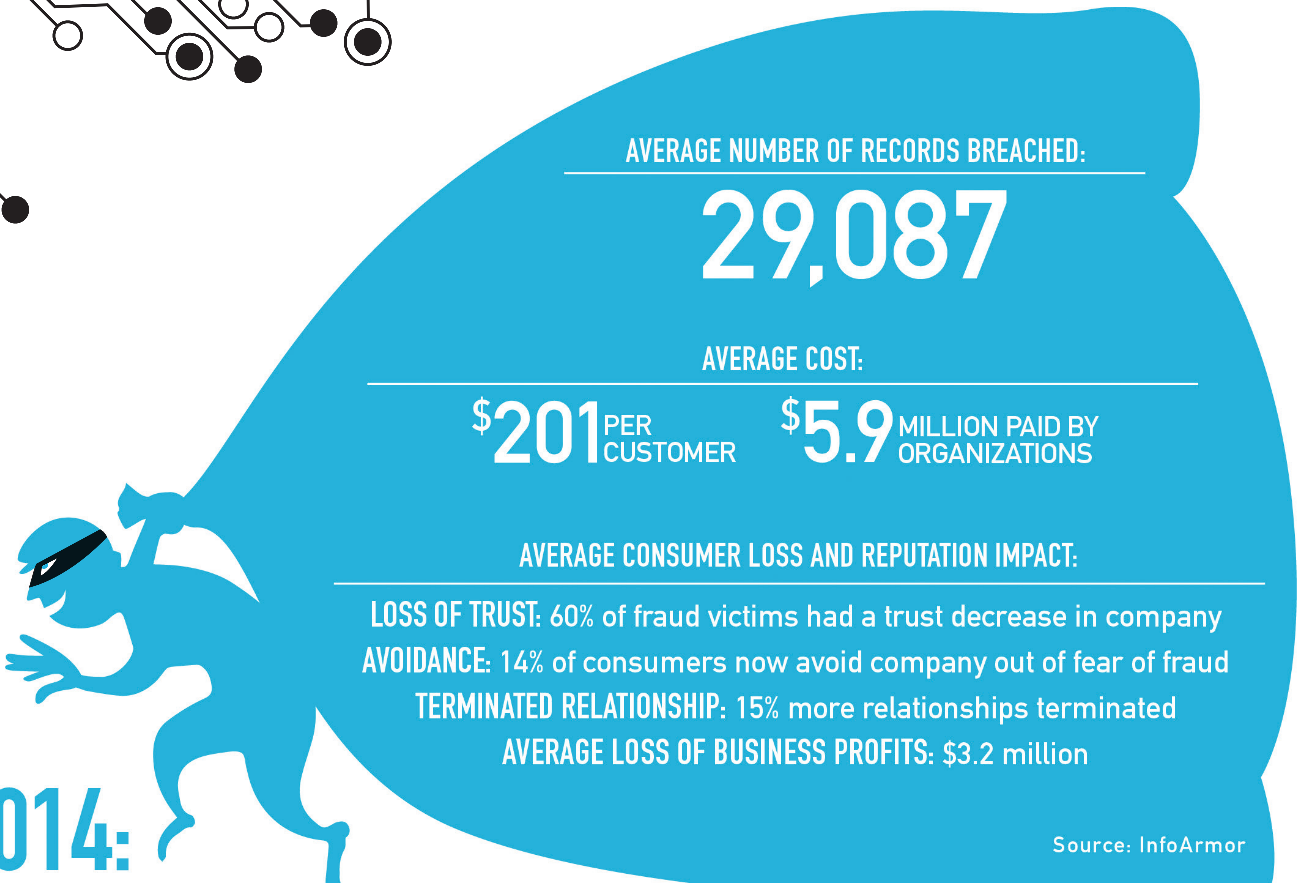
By Drew Smith, InfoArmor

Supplemental health insurance, vision care, financial counseling … and identity theft protection?

Identity theft protection is a voluntary employee benefit that is gaining in popularity among large and small firms alike. The reason is simple: nine out of 10 Americans worry about having their identities stolen, and the growing incidence of identity theft (more than 13 million Americans fell victim to these crimes in 2013, according to Javelin Strategy & Research), proves that their concern is warranted.

Employer Impact: Lost Productivity

In addition to turning victims' lives upside down, employers also feel the effects of identity theft in the form of lost productivity. Consider that employees spend up to 165 hours of work time remediating their situation. Those victimized by identity theft also are absent from work five times more than average, use medical benefits four times more than average and use twice as much sick time as



AVERAGE NUMBER OF RECORDS BREACHED:

29,087

AVERAGE COST:

$201 PER CUSTOMER

$5.9 MILLION PAID BY ORGANIZATIONS

AVERAGE CONSUMER LOSS AND REPUTATION IMPACT:

LOSS OF TRUST: 60% of fraud victims had a trust decrease in company

AVOIDANCE: 14% of consumers now avoid company out of fear of fraud

TERMINATED RELATIONSHIP: 15% more relationships terminated

AVERAGE LOSS OF BUSINESS PROFITS: $3.2 million

Source: InfoArmor

2014: THE YEAR OF THE BREACH

an average employee, according to an LSK Associates Study.

A seemingly endless stream of high-profile security breaches involving big names such as Sony, Target and even the U.S. Postal Service have spawned massive amounts of free advice about how to avoid becoming the target of an identity theft scam. But in this data-driven world, it is difficult — if not impossible — to prevent this 21st century crime.

Rather than look for ways to stop identity theft from happening at all, it is more prudent to help your employees think of detection as the new prevention.

Everyone Is at Risk for Identity Theft

Not long ago, identity theft was regarded as a problem that happened to someone else. But today, with an identity stolen every two seconds in the United States, that couldn't be further from the truth. Data and security breaches are at an all-time high. Hacking has evolved from something a computer geek may have tried in a basement to a lucrative, underground profession. In addition to becoming more sophisticated, hackers are more efficient, too. Instead of infiltrating thousands of computers to get one-off information, they are targeting one system or company to gain access to millions of identities.

The threat of having one's identity stolen is more real than ever. For many, the devastating effects still linger long after fraudulent purchases are made using unsuspecting victims' credit cards, email addresses and more. In short, the problem is reaching epidemic proportions, with perpetrators using swindled information to get everything from tax refunds and jobs to mortgages and medical care.

Unfortunately, individuals aren't the only victims of identity theft; companies bear a major cost of the problem, too. Home Depot estimates a cost of $62 million and possibly more for its breaches, while Target documented a cost of $148 million in its second-quarter filing relative to its holiday 2013 data breach. Even Sony was aware of hackers downloading gigabytes of data dating back to 2011 and spent upward of $1 billion to have an outside firm help plug the holes.

But if a company with the size and resources of a motion picture giant can be breached despite its seemingly tight security measures, what does it say for the dangers that most other companies face?

Breaches of this nature wreak unimaginable havoc. In the case of Sony, not only did the hack attack erode customers' trust in the company, it also threatened sales of its products, including a promising new Internet TV service that was set to launch last fall.

The unfortunate reality is that cyber attacks are becoming more commonplace and they cost companies more money than they realize. Companies take an indirect hit when identity thieves attack individuals because employee absenteeism rises and productivity plummets as they struggle to deal with the aftermath. The proof: victims of identity theft spend an average of 59 hours restoring their personal information and compromised credentials, and most of this time is spent during an 8-to-5 workday, as reported by the Identity Theft Resource Center's "Identity Theft: The Aftermath" report.

But that's not all. The gateway to an individual's identity records is often through their employer's corporate data security system. Employees who did their holiday shopping from their office computers and used their work email addresses as a point of contact for their purchases opened the floodgates to their firms' personnel records and other confidential information, raising the risk for both the individual and anyone with information stored on that company's network. As the saying goes, it only takes one bad seed to ruin it for everyone else.

How to Detect ID Theft Early

If there's a glimmer of hope, it's that new identity theft detection methods are helping find and rectify the problem sooner and without lasting consequences. That's a win-win for identity fraud victims who can minimize their time away from work and also for employers who can quickly and efficiently resolve the effects of data breaches to their firms.

This type of monitoring is increasingly being offered by companies as a voluntary employee benefit. It helps detect theft by alerting individuals to suspicious high-risk transactions and applications (e.g., new telecom accounts, payday loan applications and online account openings) occur. The idea is to search proactively for information misuse to reduce the damage caused by identity theft or prevent fraudulent acts altogether. This is done through real-time surveillance of the "underground" economy. If suspicious activity is detected or sensitive information is exposed, the identity restoration process begins immediately.

This comprehensive approach to identity theft detection is in sharp contrast to traditional credit bureau-based monitoring, which informs victims once fraudulent activity impacts their credit file. In many cases, a fraudster will create a synthetic identity — pairing the victim's Social Security number with a fictitious name — that goes completely undetected. The problem is exacerbated when the affected individual doesn't become aware of the situation until the malicious activity is posted to his/her credit file. That's when the time-consuming process of recovery begins.

HR, Benefits and IT to the Rescue

Without a doubt, harvesting identities is lucrative and the methods used are evolving at a breakneck pace. Individuals and companies may want to be more proactive and not only offer ID theft protection, but educate their workers about risks.

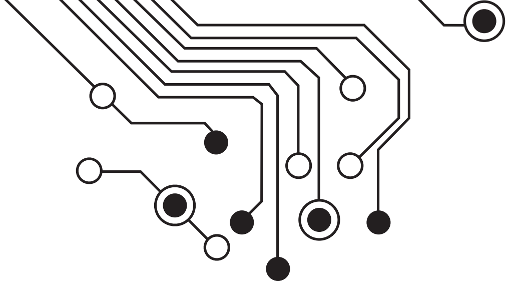
What benefits and other HR professionals can do is to gain a better understanding of the issues at hand, and employ cutting-edge privacy management solutions, to tackle this growing issue head on.

Drew Smith is founder and CEO of InfoArmor in Scottsdale, Ariz. He can be reached at drewsmith@infoarmor.com.

resources plus

For more information, books and education related to this topic, log on to **www.worldatwork.org** and use any or all of these keywords:

- ID theft protection
- Voluntary + benefits
- Benefits.



Tips to aid companies and their employees in privacy and ID fraud protection

1 Enforce mandatory password updates. Employers can protect their employees and their corporate infrastructure by requiring a mandatory password reset every 90 days (at a minimum). Allow only complex passwords that include at least eight letters, numbers and symbols. Also consider blacklisting common passwords such as "password123" or "mypassword." Instead, encourage employees to use a unique password for every personal and work-related account.

2 Use of encrypted email communication. Any email that includes personal information or intellectual property should be encrypted. Select a trusted email encryption software that is compatible with the company's corporate email solution. A hosted solution will require both the sender and recipient to be logged in to a secure portal to decrypt the message.

3 Provide identity protection as an employee benefit. Many progressive organizations offer identity protection as part of their innovative benefits package. This benefit has become a staple in the marketplace and signals value to employees. Many providers offer an employer-sponsored or voluntary benefit available through direct bill or payroll deduction.

4 Have a breach plan in place. In preparation for a data incident, it is important to put protection measures place. Such measures should be pre-determined well before an incident occurs.