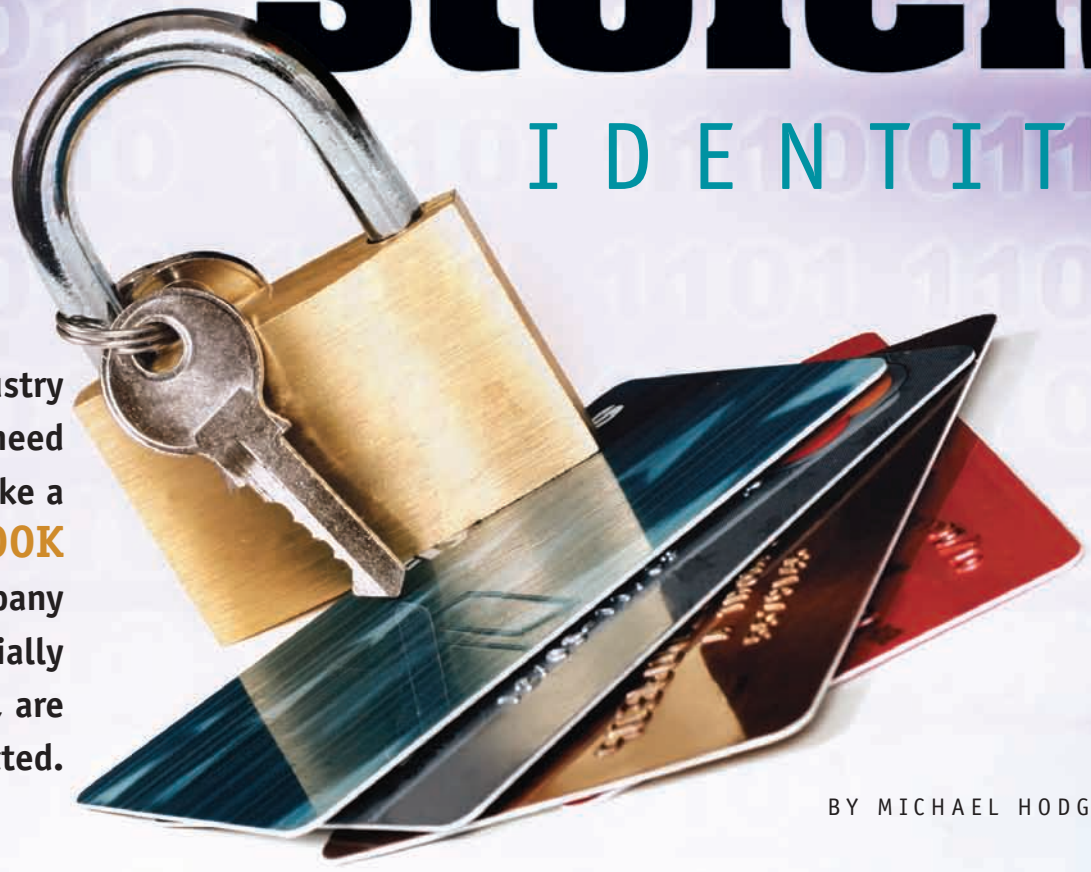
stolen IDENTITY



Outdoor industry companies need to take a VERY CLOSE LOOK at how well company data, especially employee files, are being protected.

BY MICHAEL HODGSON

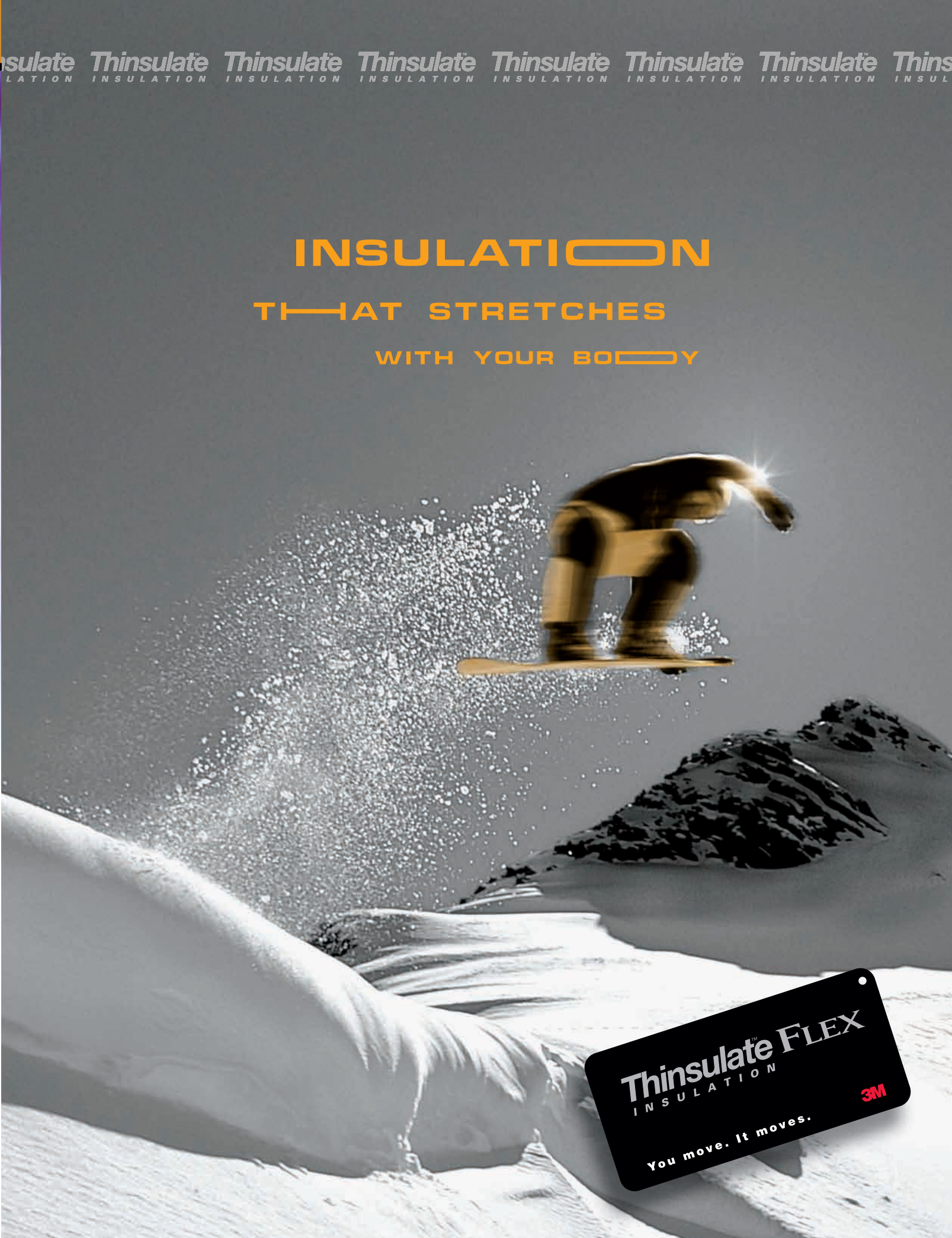
On October 16, 2005, a car was stolen in Portland, Ore. It was likely one of many car thefts that day. However, things were about to get a whole lot worse in this particular case. Inside the car was a briefcase containing payroll information for Yakima—paper files with data on every employee who had received a paycheck in 2005. The car was recovered sometime later. The briefcase was not.

Yakima's CEO Jim Clark was notified at home that evening and, within minutes, began a process that notified the Portland Police Department's fraud unit. First thing the next morning of Oct. 17, Yakima had sent an email notice to all current employees notifying each of them that a report from the payroll database containing Social Security numbers had been stolen from a car.

Working with its insurance agency, Yakima also immediately contracted with Kroll, a risk consultancy company specializing in corporate security services and identity theft—*www.krollworldwide.com*. Each Yakima employee was provided with access to a special 800 number, a packet of information from Kroll regarding identity theft, a copy of his or her credit report, and enrollment in a credit monitoring service for one year. And, yes, Yakima footed the bill.

While there may be a few of you reading this shaking your heads in amazement that any company would let an employee take sensitive paper files out of the office, we can assure you from our investigations that this is not an unusual practice historically. Many trusted employees, especially in the accounting departments, have and still do take payroll data home to play catch-up due to an ever-demanding workload. For Yakima, however—and we hope for any company that has read this—paper files containing employee personal data will never leave the four walls of corporate headquarters for any reason.

"There is simply no good reason for anyone to take employee files out of the company offices. Employee personal data should never leave the company. Period. The only exception to that rule is if you are contracting with another company, such as a health insurance company or a payroll processing company. But if you are, do you know how those third parties are handling and protecting your employees' personal information?" said Jay Foley, founder of the Identity Theft Resource Center (ITRC), a non-profit organization based in San Diego, Calif.


Thinsulate™ INSULATION
INSULATION
THAT STRETCHES
WITH YOUR BODY
Thinsulate™ FLEX
INSULATION
3M
You move. It moves.

THE COST OF IDENTITY THEFT

A Federal Trade Commission (FTC) survey in 2003 revealed that 27.3 million Americans had been victims of identity theft in the last five years, including 9.9 million people in 2002 alone. According to the survey, 2002's identity theft losses to businesses and financial institutions totaled nearly $48 billion and consumer victims reported $5 billion in out-of-pocket expenses.

Businesses are affected each time an identity thief misuses an existing account or opens a new account in the names of victims to purchase products or services, rent apartments and homes, obtain medical care, seek employment, obtain fake government documents or commit other frauds.

Employee productivity can be affected too when identity theft strikes. The FTC survey found that victims on average spent up to 600 hours trying to resolve identity crime, which can take a toll on productivity as well as morale at the workplace.

Businesses may unwittingly hire criminals who apply for jobs, using the names, credit and work histories of reputable workers. Surveys in 2003 and 2004 by ITRC found that employees were sometimes victims of identity theft at the hands of current or former employees of their company.

MORE VULNERABLE THAN YOU IMAGINE

As a part of a random and casual phone survey of key executives at a variety of outdoor companies around the United States during November 2005, GearTrends® was frequently told that what happened to Yakima could never happen because each had a very strict policy regarding the protection of company employee files and information. And yet, when we brought up laptops, asking about confidential company files, confidential information about clients and more, in nearly every case, it became very clear that laptops were a ticking time bomb.

"If I lost my laptop, I'd be in serious jeopardy—it is loaded with confidential files and client data," said one corporate executive with whom we spoke. "I am going to immediately check in with our IT people to see about what we can do to encrypt or protect all of our company laptops."

According to Safeware, a provider of specialized insurance programs for computer, electronics and high-tech equipment owners, more than 600,000 laptops are stolen or lost every year, increasing the risk of confidential customer data, corporate trade secrets and classified documents becoming compromised.

Kroll, the risk consultancy company, strongly recommends in one of its company website pages on protecting against corporate identity theft that businesses "develop an encryption system for computer-based information and evaluate its effectiveness regularly."

With a good encryption program, even if an intruder manages to break through a company firewall, the data on the network can be secured if it is encrypted. Standalone encryption packages that work with individual applications are in the public domain and available for sale.

One such program, and one that Foley uses on his own computers, is offered by CyberAngel Security Software (*www.thecyberangel.com*).

According to Foley, CyberAngel creates what amounts to a separate and secure hard drive (partitioned) on a computer that houses all confidential data, encrypting everything inside that

ARE YOU PROTECTED?

Take a few minutes to take the following quiz, created by the Identity Theft Resource Center. It will help you determine just how effective the company you are working for is at keeping your personal information safe. Answer "yes" or "no" to each of the following:

- Your company conducts a criminal or civil background check before hiring employees who will have access to personal identifying information.
- Your company provides cross-cut paper shredders at each workstation or cash register area or uses a locked wastebasket and shredding company for the disposal of credit card slips, unwanted applications or documents, sensitive data or prescription forms.
- Your company uses an alternate number instead of a Social Security number (SSN) for employee, client and customer ID numbers.
- Your company never sends out mail that includes your complete SSN.
- Your company requires its health insurance providers to use an alternate number rather than the SSN for membership numbers on health insurance cards.
- Your company has trained designated staff about security procedures in sending sensitive personal data by fax, email or telephone.
- When you are in the public areas of the company, you cannot see the sensitive information of consumers or employees on any item (timecards, badges, work schedules, licenses, etc.) that may include home address or phone numbers, SSN and driver's license number.
- In the event of a computer breach of a database (or loss of paper files) that contains sensitive information, affected individuals are notified in a timely manner.
- If your company requests a customer give it an item for security (for example, to get a locker), the item is not a driver's license, Social Security card or other card with identifying information.
- Your company places photos on employee business cards for better identification and security.
- Your company keeps all paper files and personal data about employees and customers in locked cabinets.
- Your company encrypts or password-guards all sensitive data stored on computers, and it allows access only on a "need-to-know" basis.
- Your company has trained employees in how to receive personal identifying information from customers and clients without jeopardizing their security. For example, staff never repeats a customer's credit card number or expiration date loudly in a crowded store if taking an order over the phone.
- Consumers and employees are notified in advance as to the purposes of the data collection, to whom it will be distributed and the subsequent use after the fulfillment of the original purpose.
- Your company never asks for more data than absolutely necessary.

If a majority of your answers to the questions above were either "no" or "maybe," perhaps it is time for you to speak up at work and demand your company does more to protect not only your personal data, but all personal data collected.

NATIONAL MOLDING CORP. PRESENTS THE...

DURAFLEX INVASION '06

FEATURING ITS NEW MESHTEK™ SERIES

VEE BUCKLES

LONG TAB MESHTEK™ TENSIONLOCK®

SCREEN VEE BUCKLES

SHORT TAB MESHTEK™ TENSIONLOCK®

DUAL ADJUSTABLE MESHTEK™ ROCK LOCKSTER

MESHTEK™ ROCK LOCKSTER

Over the past 20 years, National Molding has established itself as the preeminent source for buckle hardware to the outdoor industry.

Continuing our history of product innovation, we now introduce our new Meshtek® series.

BUILT TOUGH, RUGGED AND DURABLE FOR TODAY'S OUTDOORS.

DURAFLEX®

SPECIALTY BUCKLE & FASTENER HARDWARE BY NATIONAL MOLDING CORPORATION

5 Dubon Court, Farmingdale, NY 11735-1065 • 1-631-293-8696
1-800-544-7162 • Fax 1-631-293-0988 • www.duraflexbuckles.com

drive partition preventing unauthorized access to your files, company financials, client information or corporate business plans.

If your computer is stolen and the log-in authentication is violated at start-up, all sensitive data and information is protected as well as rendered invisible to that unauthorized user. In addition, the stolen computer begins to, without the thief's knowledge, send wireless or modem communications to the CyberAngel security center that will then communicate with law enforcement regarding the computer's location. It's tantamount to your computer yelling for help.

Case studies and write-ups of recent arrests on the CyberAngel site indicated that thieves are more than a little surprised when the police come knocking.

WHAT SHOULD YOU DO?

If you have reason to believe your personal information has been stolen, and especially if information containing your Social Security number has been lost or stolen, you should first call your local police department and file a report. Get a copy of that report, as creditors will require that report before absolving you of any fraudulent debts.

Next, file a complaint with the FTC online at *www.consumer.gov/idtheft* or by calling 877-438-4338. This step adds your report to the FTC Identity Theft Clearinghouse and becomes accessible by law enforcement officers for use in investigations.

Naturally, you will want to contact your bank, your credit card companies, and the three major credit bureaus—Equifax (800-525-6285), Experian (888-397-3742) and TransUnionCorp (800-680-7289).

Finally, for more information on the subject of identity theft ideas for better safeguarding information, go to the Better Business Bureau's ID theft pages at *www.bbbonline.org/idtheft*.

MORE RESOURCES AT-A-GLANCE

» *A PDF guide on ID theft from Privacy and American Business: www.bbbonline.org/IDtheft/PABIDTheft.pdf*

» *Tips for consumers and businesses on staying safe online from GetNetWise: http://security.getnetwise.org*

» *Banners and button images your business can display to affirm it is committed to protecting against ID theft: www.bbbonline.org/IDtheft/banners.asp*

web extra

For more information on safeguarding your company information, an added benefit for GearTrends® magazine readers, go to www.geartrends.com/extras.

HOW SAFE IS YOUR INFO?

Jay Kroll, founder of the non-profit Identity Theft Resource Center, will come into the workplace and, for a $4,000 fee, work with a business to help it determine ways it might need to tighten up and batten down to ensure data and personal information is as secure as humanly possible.

Kroll told GearTrends® that it is only by learning to handle all company information safely can a company hope to keep personally sensitive information out of the hands of criminals.

He offers the following quick list of questions for each industry segment—retailer, rep, distributor, manufacturer, supplier—to use as a starting point for improving security:

» **Information acquisition:** Do you have a good reason for requesting the information that you gather? Are you acquiring it in a safe manner so that it cannot be overhead or seen by others?

» **Storage:** What computer security measures have been placed around the systems storing personal data? Is the data considered highly classified and not common access?

» **Access:** Is personal identifying information available only to limited staff? Is database access audited or password-controlled?

» **Disposal:** What is in your dumpster? Is it a treasure chest for thieves? Are electronic/paper documents and databases containing personal information rendered unreadable prior to disposal?

» **Distribution:** Are all of your employees trained in the proper procedures regarding information disclosure? Do you publicly display, use or exchange personal information (especially Social Security numbers) in your workplace? This includes employee or membership cards, timecards, work schedules, licenses or permits, and computer access codes.

» **Personnel:** Do you conduct regular background checks on ALL employees with access to identifying information? That might also include mailroom staff, cleaning crews, temp workers, and computer or hotline service techs.