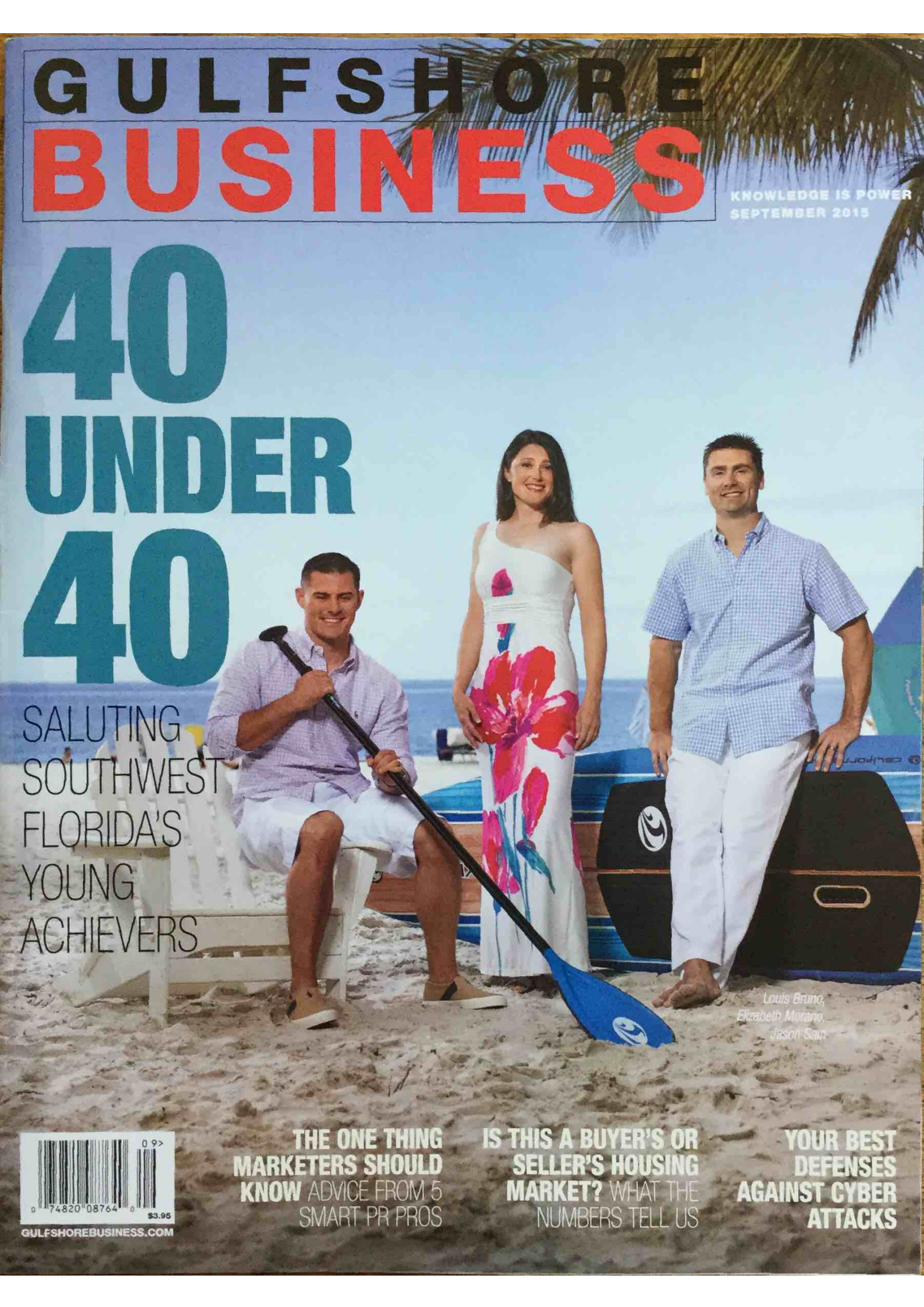
GULFSHORE BUSINESS

KNOWLEDGE IS POWER
SEPTEMBER 2015

40 UNDER 40

SALUTING SOUTHWEST FLORIDA'S YOUNG ACHIEVERS



Louis Bruno,
Elizabeth Morano,
Jason Saul

THE ONE THING MARKETERS SHOULD KNOW ADVICE FROM 5 SMART PR PROS

IS THIS A BUYER'S OR SELLER'S HOUSING MARKET? WHAT THE NUMBERS TELL US

YOUR BEST DEFENSES AGAINST CYBER ATTACKS

09>
0 74820 08764 0
$3.95
GULFSHOREBUSINESS.COM

STARTUP STORIES, CONT.

gram—which focused on teaching Polish—the company added new languages quickly after establishing that initial template. The wide variety of languages differentiates Dino Lingo from its competitors, Acar says, in addition to the fun, kid-focused curriculum that Acar says is ideal for children from 1 to 8 years old. "We have a social mission," he says. "We believe anybody in the world, if they want to learn a language, they should be able to find the proper materials for it."

WHAT'S NEXT

Dino Lingo includes two full-time employees in addition to Acar, who says his company is profitable and generated about $600,000 in sales last year. He predicts revenue will rise to $750,000 this year and will go even higher to $1.5 million the following year as a result of several new products—including a program geared for adults—that should be available soon.

So far, Acar and his wife have self-funded the business. But they eventually plan to seek outside investment. He says the company has strong potential, even suggesting it could become a billion-dollar business. "If we keep adding new products, new services, new languages, I'm sure the customers will love it," he says.

—Dave Ghose

BEST PRACTICES

SIX STEPS FOR TIGHTER CYBER SECURITY

If you think your business is secure because you have an alarm system and security cameras, think again. As technology advances, so do the ways in which your company can be harmed. Hackers and malware—a sneaky code that can create viruses and other software that disrupt a computer system—present real threats. Hackers can access sensitive data from across the world with just a few clicks and keyboard commands. Small- to medium-sized businesses can be easy targets.

"They know these businesses don't have the funding or IT departments," says Carrie Kerskie, author of *Your Public Identity: Because Nothing is Private Anymore* and president of Kerskie Group, a cyber security protection firm in Naples. "Small businesses have been the No. 1 target—they're the low-hanging fruit." Protecting the integrity of customer information is one of the biggest components of a successful business, says James Hansen, president and chief executive officer of Black Eagle Security Team, a cyber security and solutions provider in Naples. Kerskie and Hansen shared the basics of cyber security and how to keep your information safe.

INVEST IN EMPLOYEE TRAINING

Savvy employees are crucial to helping identify phishing emails in which hackers disguise themselves as a trustworthy entity to obtain personal information, and knowing if a link will lead to malware that can crash a computer. "The one thing about data privacy training is that telling employees what not to do is not effective," says Kerskie, who is also director of the Identity Fraud Institute at Hodges University. "The only way you can really make an impact is by having them change their habits and help them understand the flow of information."

CONDUCT A RISK ASSESSMENT

In 2012, more than 2,500 cyberattacks were reported to PricewaterhouseCoopers (PwC). By 2014, this number had risen to more than 4,000. How does your business fare against your competitors?

Kerskie suggests conducting a risk assessment in which you identify the strengths and weaknesses of your business and its hardware, software and data policies. It is also important to have a firm understanding of how your company's personal information flows throughout technology.

CREATE A DATA MATRIX

Data matrixes sound complicated, but they're really fancy spreadsheets for information, showing what information you have and where it's stored—a vital aspect of cyber security. "The level of a data breach can

BEST PRACTICES, CONT.

be determined by what information was potentially exposed," Kerskie says. "In the event you do get a virus, you, then have to be able to identify which files were accessed, and if you don't have a data matrix, you have to access each folder and check."

CHANGE PASSWORDS FREQUENTLY

Sure, it's frustrating to remember a laundry list of passwords, but passwords should be tighter than Fort Knox. "Businesses really need to get away from master passwords," Kerskie says. "The reason you want different usernames and passwords is to look at the login data and see what user credentials accessed the sensitive information—without this, there's no accountability." Kerskie recommends changing passwords at least every six months, and making the password 12 characters or more, as the old standard of six just isn't good enough these days.

DILIGENTLY SCAN YOUR IP ADDRESSES

An IP address is basically a group of numbers that identifies a piece of technology and allows it to communicate with other devices. Hackers use IP addresses to trick technology and allow the hacker into their system.

"For anything to work on your network, it has to have an IP address," Hansen says. "One of my clients had given the printer full administrative rights to the system, so all you have to do is log in through the printer's IP address and you have complete access to the system and its information." Carefully read over the settings of your technology to avoid these situations.

KNOW WHOM TO CALL WHEN YOU'VE BEEN ATTACKED

"People ask if I can guarantee they will not be attacked if we put certain countermeasures in place," Hansen

says. "So I ask them three things: Who will attack you, when will they attack you, and how will they attack you?" Of course, no one can answer these questions. The point of cyber security providers isn't to avoid all attacks, but to minimize and mend them if they occur. It is vital for a business to be able to call a third-party resource for assistance when disaster strikes. "It's a very complex issue, and there isn't a silver bullet or single answer," Hansen says. "But there's no such thing as being totally protected."

—Hunter Lacey

THE ART OF SELLING

CROSSING THE BARRICADE

In last month's column, I wrote about the need for salespeople to be bold at times, using an example from a recent U2 concert I attended. At that same show, there was a second highlight that helps to illustrate another important lesson that I'd like to share.

During one of U2's songs in their live concert, there is an interlude where Bono has a fictional conversation with himself, where the Bono of today is speaking to the Bono of age 19. This conversation has been folded into the song and contains an important modern twist. To really capture the audience's attention, Bono uses a bullhorn and shouts into the microphone "I'm on the other side of the barricade now! I'm on the other side of the barricade now!" He then continues without the bullhorn "I'm on the other side