
BAYLOR BUSINESS
review
FA
06
BUSINESS+
TECHNOLOGY
BaylorBusiness
Hankamer School of Business

BY BARBARA ELMORE

01010THE1GRAYOSIDE

When the computer language BASIC emerged almost half a century ago, the phrase cyber warfare wasn't in the dictionary and the word virus was often preceded by flu. Blackberries were a fruit, telephones didn't play music and Spam came in a can.

Now, using spam as bait, computer tricksters "phish" online for new identities. Scam Web sites, purportedly charities, go up for a few days to take your money and run. Trojan horses carrying poisons try to invade your computer's defenses. Someone out there just might be trying to capture your personal information by recording your keystrokes, and a new industry has developed around virus software and anti-spyware.

Is there a solution to these technological difficulties, short of logging off for good?

Yes, say the experts who have grown their skills as the technology blossomed. They're likely to advise us to be more wary of human error than human evil. After that, they emphasize the value of setting priorities on what we want to keep private. And to plan for inevitable surprises.

Baylor professor and computer security guru Randal Vaughn puts the darker side of technology into perspective with the notion that both white hats and black hats populate the world, "and most people are kind of gray." Much of the mischief done through technology comes from human error, he said, not deliberate evil.

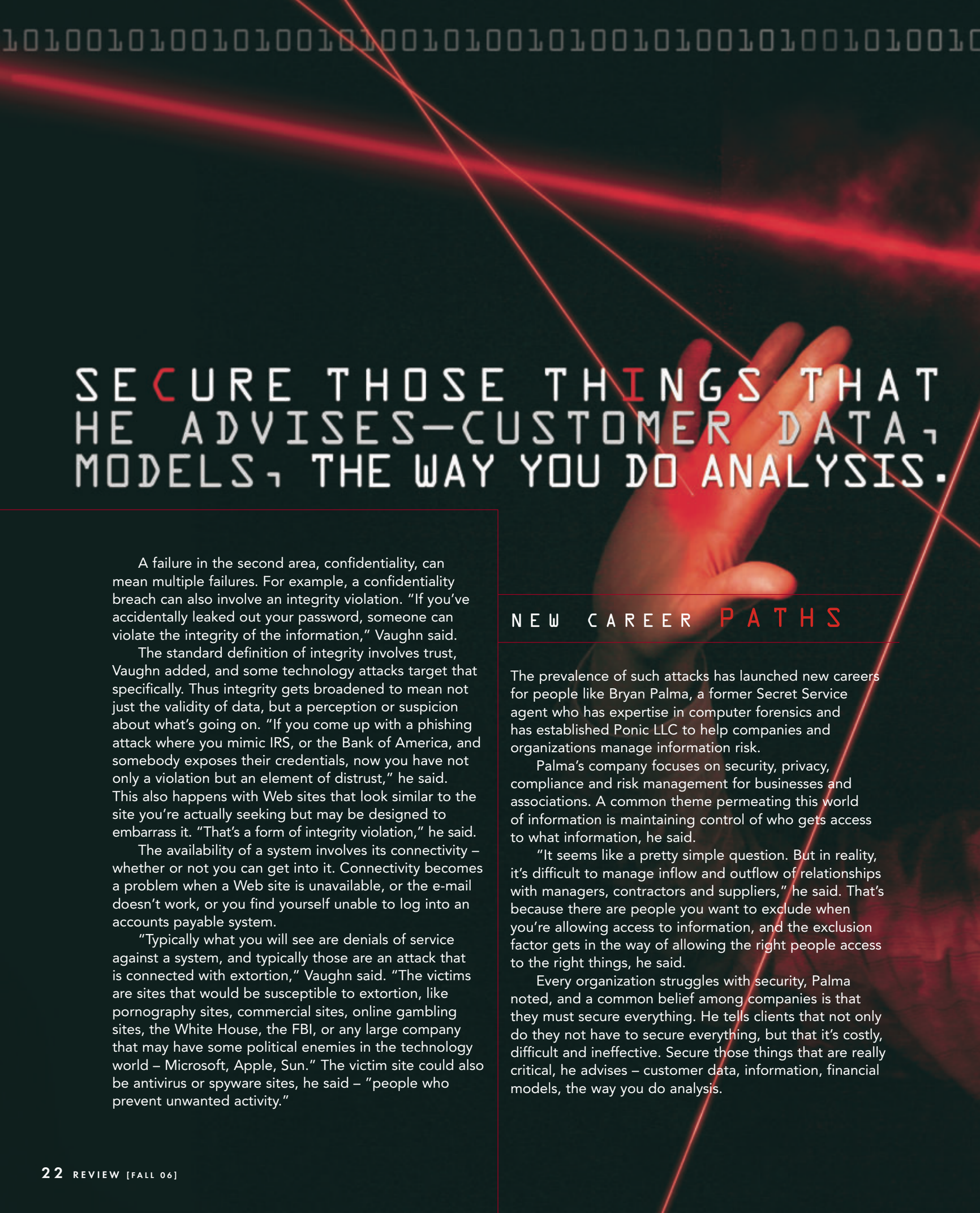
BEWARE HUMAN ERROR

Vaughn, professor of Information Systems, is well-versed in computer viruses, cyber warfare, phishing and the poisoning and destruction of data. His expertise comes from running the Baylor business school's operating system years ago as well as spending time as a project engineer for the Air Force and working for Vought Aircraft and Mobile Oil. Experience has taught him that the most popular way of crippling a business is by "plain old human foul-up."

"In the security world we teach students that our number one vulnerability is our own people," Vaughn said. "They just mess things up." They make mistakes typing in data, or they accidentally delete key information.

He leads classes in the basics of technology and policy issues as well as a graduate-level course in cyber warfare. Computer security must cover three main areas, Vaughn noted. These include integrity in the system, or whether people trust it; confidentiality, or whose eyes see it; and availability, or how easy it is for users to access.

An operating system's integrity can be compromised by the aforementioned human foul-up or by external attack, such as poisoning or destroying data. And whether the integrity is violated accidentally or on purpose, security checkers can look for ways to see if the data has changed. But tracking is difficult, he said, and sometimes impossible.



SECURE THOSE THINGS THAT HE ADVISES—CUSTOMER DATA, MODELS, THE WAY YOU DO ANALYSIS.

A failure in the second area, confidentiality, can mean multiple failures. For example, a confidentiality breach can also involve an integrity violation. "If you've accidentally leaked out your password, someone can violate the integrity of the information," Vaughn said.

The standard definition of integrity involves trust, Vaughn added, and some technology attacks target that specifically. Thus integrity gets broadened to mean not just the validity of data, but a perception or suspicion about what's going on. "If you come up with a phishing attack where you mimic IRS, or the Bank of America, and somebody exposes their credentials, now you have not only a violation but an element of distrust," he said. This also happens with Web sites that look similar to the site you're actually seeking but may be designed to embarrass it. "That's a form of integrity violation," he said.

The availability of a system involves its connectivity – whether or not you can get into it. Connectivity becomes a problem when a Web site is unavailable, or the e-mail doesn't work, or you find yourself unable to log into an accounts payable system.

"Typically what you will see are denials of service against a system, and typically those are an attack that is connected with extortion," Vaughn said. "The victims are sites that would be susceptible to extortion, like pornography sites, commercial sites, online gambling sites, the White House, the FBI, or any large company that may have some political enemies in the technology world – Microsoft, Apple, Sun." The victim site could also be antivirus or spyware sites, he said – "people who prevent unwanted activity."

NEW CAREER PATHS

The prevalence of such attacks has launched new careers for people like Bryan Palma, a former Secret Service agent who has expertise in computer forensics and has established Ponic LLC to help companies and organizations manage information risk.

Palma's company focuses on security, privacy, compliance and risk management for businesses and associations. A common theme permeating this world of information is maintaining control of who gets access to what information, he said.

"It seems like a pretty simple question. But in reality, it's difficult to manage inflow and outflow of relationships with managers, contractors and suppliers," he said. That's because there are people you want to exclude when you're allowing access to information, and the exclusion factor gets in the way of allowing the right people access to the right things, he said.

Every organization struggles with security, Palma noted, and a common belief among companies is that they must secure everything. He tells clients that not only do they not have to secure everything, but that it's costly, difficult and ineffective. Secure those things that are really critical, he advises – customer data, information, financial models, the way you do analysis.

Privacy is important to consumers who want to do business online, Palma said, and important to building the trust relationship that Vaughn talks about. "Citizens and consumers are saying, 'If you want me to participate in online commerce…make assurances that you are protecting my data,' " he said. Once again, information risk concerns are related. "You can't have privacy without security," Palma noted. "Privacy can drive better security, and companies will take notice when customers say, 'We aren't accepting the procedures that we did before because we don't think they protect our information.' "

He applauds the United States' free-market approach to data collection as long as laws protect personal information like Social Security numbers.

BRYAN PALMA

"People want different things online, and there are all kinds of things in between the 401K account and the chat room. To me that's the place that the average person and a lot of organizations are overlooking. If you can fix the inclusion, it makes the exclusion a lot better as well."

HAVE A PLAN

If you want to guarantee technology's best uses, plan it and test it, said Anita Knight, founder of the Knight-Star Institute. She saw the value of strategic planning after executing a year-long disaster plan within the New York insurance industry immediately before Sept. 11, 2001.

"I was a team leader for a cross-functional, industrywide team of insurance people," Knight said. "We'd been in the process of creating a plan for the state of New York that ensured we could cooperate with each other and the state emergency response and regulatory community." Her team had just finished the planning process when 9/11 happened.

The blueprint she helped create put her in charge of activating the emergency plan with the insurance commissioner of the state. She and one of his employees put it into action when the commissioner himself was "running for his life in Manhattan." Insurance catastrophe specialists flew into Albany, and the group spent weeks after the attacks toppling barriers so that people could get the insurance they needed to live.

This was no small feat for the competitive insurance industry, Knight said. The planning made it work. After it was over, government agencies, trade organizations, and the state regulator's office examined the response and rated it the best of its kind, she said.

Knight moved to Central Texas and opened her own Homeland Security consulting firm, Knight-Star, four years ago. Now the organization is using a FEMA grant and training fees to provide grassroots community education to ensure regional readiness. The firm employs trainers, consultants, critical event responders and advisers who are experts at thinking about catastrophes in advance so they can manage the aftermath. Knight-Star consults with schools, hospitals, police and fire departments on disaster preparedness.

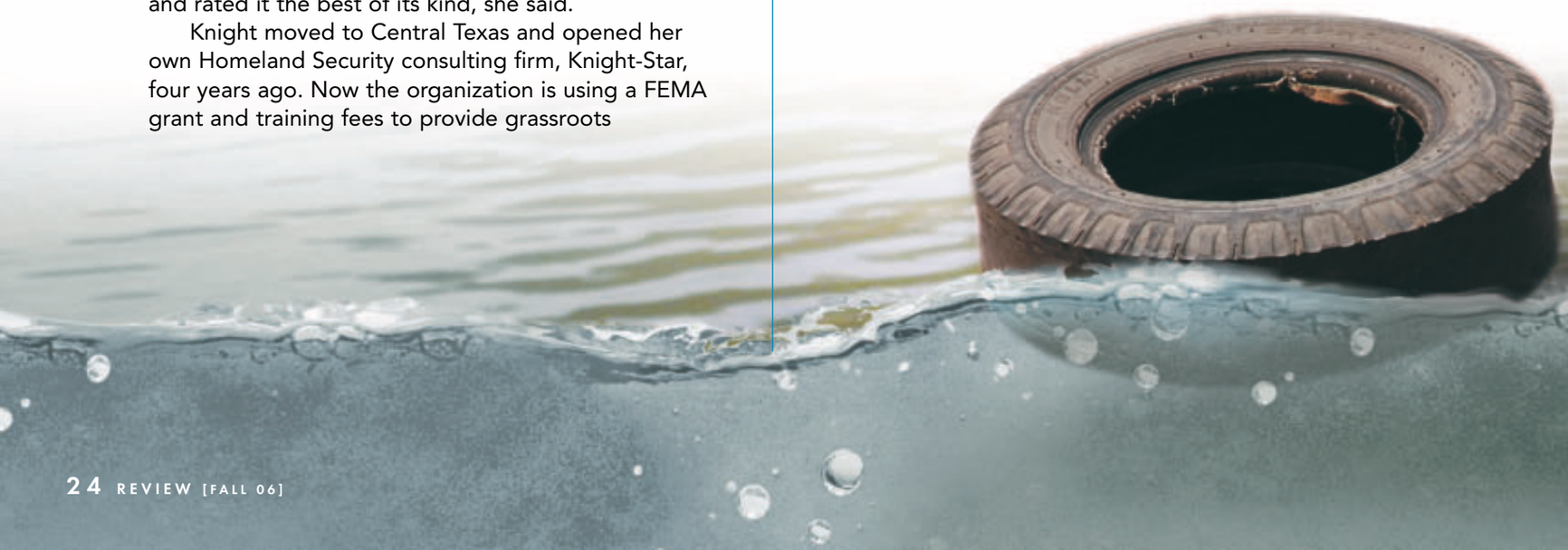
Senior vice president and vice chairman of the Knight-Star board Robert L. Clark, a former military officer who has served worldwide, said he was attracted to Knight-Star by his concerns about terrorism. "I looked at what Knight-Star was trying to accomplish and found this niche, which includes developing programs for schools and hospitals."

Clark is working with public schools on a program to analyze their emergency plans and conduct an orientation program to introduce the schools and community leaders to the National Incident Management System, which empowers government and non-government agencies to work together during domestic crises. Knight-Star is also helping the schools evaluate and test their emergency plans.

The company offers a free "Masters of Disaster" teacher-trainer workshop to teachers and other school staff so they can learn how to implement a grassroots safety and preparedness curriculum for students. The workshops are based on a Red Cross curriculum.

"It's part of the FEMA grant," Clark said. "We train the trainers, teachers, train children, train families." Knight-Star also leads workshops for nursing homes and residential care facilities and provides similar services to health departments.

THE PLANNING MADE IT GOVERNMENT AGENCIES, TRADE REGULATOR'S OFFICE EXAMINED THE BEST OF ITS KIND.



Knight's work on disaster planning brought her to Baylor when Anne Grinols, assistant dean of faculty development, asked her to talk to students about crisis communications. "As we started talking, she shared with me that she wanted to get her students to Washington, D.C., and get more involved in government activities," Knight said. "We realized then we could collaborate and do something fairly important for rural schools."

Baylor student Tony Trippodo worked with Knight-Star as part of a Baylor Focus Firm project, Project Vigilance, that students presented to government officials in Washington, D.C., last April. "I was part of a team of 15 people," Trippodo said. He studied logistics for preparedness, including emergency procedures for parents to know what to do when a disaster strikes, such as pre-designed places to pick up children who have been evacuated.

"We looked at best practices for school disaster plans," Trippodo said. "They are pretty limited. This is a big plus for Knight-Star, to provide unique affordable services to help schools get their plans together. Most don't know how to do it."

Also employed at Knight-Star before graduating in August was Baylor student Douglas Franks, who worked on a U.S. Department of Education grant involving six different rural independent school districts.

WORK. AFTER IT WAS OVER, ORGANIZATIONS, AND THE STATE THE RESPONSE AND RATED IT

ANITA KNIGHT

Knight describes security preparedness as a growth industry and calls the need for it unfortunate. "Current events make it real clear that Americans are experiencing a kind of social awakening around disaster preparedness at all levels. Have a plan and have a kit—everyone needs one. That's our motto."

Vaughn, the Baylor professor, notes that attacks using new technology don't reveal any new sociological issues. The technology is simply an extension of the issues, he said. "We are actually in a competitive society. We kill off the dumb and only the smart remain, and the really smart develop new tactics against the method used to prevent their activity. It's a lot faster—instead of a scam taking hours, now you can do it on the Internet with an e-mail. But it's a different form of the same old thing."