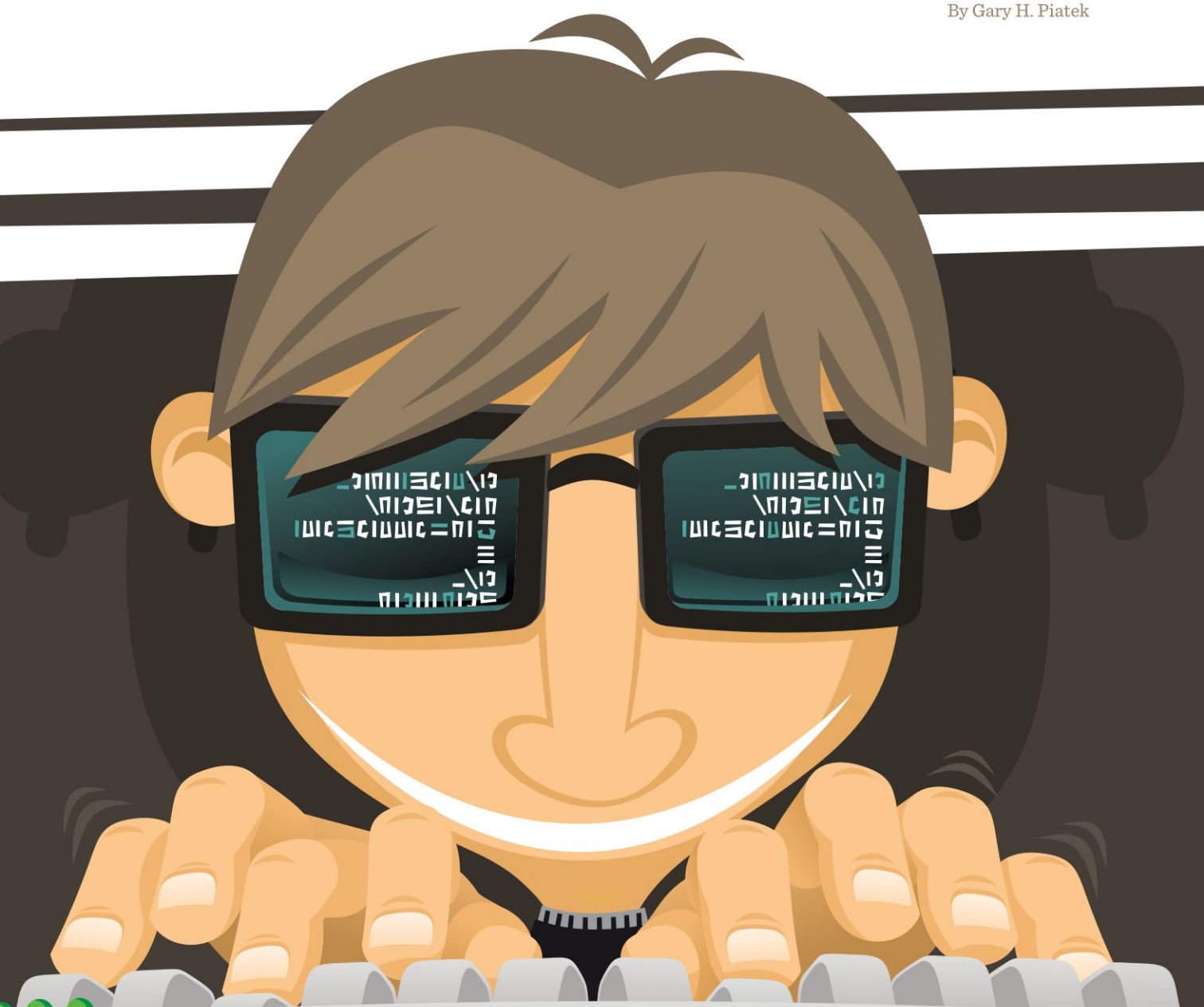
Small businesses are the hackers' sweet spot

How to protect your investment

By Gary H. Piatek



Doug Witten, Baker College's cyber defense program director, tells a funny story that illustrates just one of the dangers of being lax about cybersecurity.

When Witten worked at EDS, one of his friends was a practical joker. That guy left his computer unlocked around the Christmas holiday. Witten noticed that, went in and called up his email and sent a note to everybody in EDS throughout Flint. The note said, "I just want to let you know how much I truly love you," and put the man's name on the bottom and sent it. "He was getting emails back over Christmas break saying, 'Uh, I … love … you … too?'"

We can laugh at that, but if it had been a computer at your small business and the "practical joker" had been someone with nefarious intent, it's a good bet that you would not be laughing.

Witten gave an example of the scope and seriousness of the cybersecurity problem by recalling the nine years he oversaw the infrastructure of michigan.gov.

"We averaged 10,000 hacks a day against us," he said. "People love trying to break into the government. We had the resources to defend against that kind of stuff."

While the "big boys" of business spend millions of dollars a year on cybersecurity, many small-business owners don't realize that they are equally at risk for an attack.

But the reality is that small businesses fall into a hacker's "sweet spot," said Stephen Cobb, a senior security researcher at anti-virus software company ESET. Small businesses have many assets to target but less security than larger companies because as many as 80 percent of small companies believe they don't have anything worth stealing, according to Towergate Insurance.

Witten agrees, adding that "a hacker is just looking for information, something valuable that they can exploit: somebody's Social Security number (or) credit card numbers. Today's hackers are in it for the profit." The easier the target the better. And even if a small-business owner realizes that he could be a target for hackers, he often doesn't have the resources to have his own robust IT department. In that case, Witten and others say, a third-party security company could be the answer.

That was the case with Stat EMS LLC.

Because of the sensitive information it collects, the Flint company has had to stay on top of technology, said Matthew Rozen, director of business development.

Rather than have its own IT department, however, Stat EMS has always relied on a third party because of the complexity of its data, he said.

"We have so many spokes in our wheel, most of it patient information security."

Those "spokes" include phone calls containing personal information that move to an emergency dispatcher from a home or an accident site or crime scene. That information is then sent to the emergency vehicle where more information is gathered and then sent to a hospital or other appropriate agency, and then to the billing department.

"The connectivity and the availability of our vehicles is paramount for us," he said. "The information that needs to be protected is constantly traveling back and forth. How do we protect ourselves?

"If you don't have that capability internally, then you have to have someone you trust externally," he said.

Rozen decided to turn to Spud Software and INC Systems, both in Grand Blanc.

Jeremy Smith, senior developer at 20-year-old Spud Software, said that many small businesses just ignore security because they feel they don't have the manpower, the time or the money.

A small company should at least hire someone to do an annual audit of its systems to see if it has been hacked or if credit card information has been stolen, said Larry Bossman, sales director at Spud.

"Do a regular checkup of the network to see if there are any vulnerabilities," he said. But Bossman cautioned the business owner to first look at the qualifications of the company: what is its size, is it an established business, what is its history, check its references.

Aaron Hamp, CEO of INC Systems, agrees.

"You can't just go hire a guy who knows computers and think that you have an IT department."

He estimated that to do an IT department correctly, a company would have to spend about $250,000 a year.

"What you need," he said, "is an entry-level guy who can do the printer fixes, plug in this and that; you need a high-level engineer who understands network security, server configurations; and then you need a manager who can interface with the leadership team and translate the geek speak into business ideas."

Hamp emphasized that no matter how you tackle IT, training is key.

"People are the piece of the equation that throws everything out the window," he said. "It doesn't matter what security you have in place, if you allow the bad guys in, there's nothing we can do. So education is a big piece of cybersecurity."

Suggestions made by Witten, Smith and Hamp on how businesses can help protect their data:

1. Understand the importance and security of your data.
2. Understand the risks to you and your customers.
3. Make sure your servers are not accessible to the public.
4. Hire a company regularly to do an IT audit, and get a second opinion.
5. Hire a company to consult on setting up a system.
6. Encrypt sensitive data and hash passwords.
7. Know if your data is being backed up, and how it is being done.
8. Stay up to date with software.
9. Have a strategy to patch software holes.
10. Know who is keeping track of your network and who has access.
11. Use the "least privilege principal," which means you give all of your users just enough privileges to do their jobs. If they need elevated rights, they must go to a trained key person who doles out those rights.
12. Keep up to date with security-related training.