Cyber criminals target small businesses

By Callie Byrnes

In the 43 years that Larry McElwain owned the Warren-McElwain Mortuary, he didn't worry much about cyber thieves hacking customer information. He said that most people couldn't charge enough credit to pay for his funeral services on their cards, so it never crossed his mind that it could be a big problem for businesses around the world. It wasn't until he took his granddaughters to a restaurant in San Diego and had his own credit card information stolen that he began to realize just how important credit card security is to customers and businessmen alike.

"It's important that people know this can happen," McElwain, who has sold his business and is now the president and CEO of the Chamber of Lawrence, said. "It's unbelievable that people spend their time thinking of ways to cheat other people, but that's how it works."

Although big companies such as Target and Home Depot are under fire for large-scale information hacks that have compromised millions of customers' credit card information, small businesses are becoming the targets for cyber thieves and data hackers. According to the Wall Street Journal, the switch to computerized records and digital systems have made small businesses the main target for system hackings. However, with the larger hackings overtaking the news, the danger of information compromises in small businesses is often overlooked. Jamie Guffey, manager at the Toy Store, 936 Massachusetts St., said he hasn't worried about system hackings affecting the business.

"I guess from my shoes representing small companies, I don't necessarily see this as much as an issue," Guffey said. "I think that we're probably not as much as a target in the sense that we have less information to access."

Beau Bruns, general manager at the Burger Stand, 803 Massachusetts St., also

believes that information leaks are not a huge problem for small businesses in Lawrence.

"Fortunately, nobody's really trying to hack the Burger Stand or Sunflower Bikes or Henry's Coffee Shop because the amount of credit card information we have is tiny," Bruns said. "The probability of the Burger Stand getting hacked and losing a bunch of customer's credit card information is probably slim to none."

However, the Wall Street Journal reported that the size of the business isn't the only thing that hackers consider. Instead, it is the strength of the security systems that the businesses have. Of the 761 data breaches reported by the U.S. Secret Service in 2010, 482 were at small companies of 100 employees or fewer.

According to Jamie Lowe, owner of Prairie Land Insurance on 123 W. 8th St., the misconception that small businesses are not at risk for cyber theft has to do with the fact that most data breaches go unreported. He estimated that approximately 10 percent of all data breaches go reported.

"If that happens to your business, you don't want the public to know that," Lowe said. "You're not going to try to draw attention to yourself because it's an embarrassment to you and it could jeopardize your successfulness in your community."

McElwain thinks that these breaches in privacy will only become more prevalent as new technology develops.

"I think the iPhone invention has opened the floodgates because the capabilities of that device," McElwain said. "I mean, they're saying that people can copy smart phone information by standing next to you in a crowd, and I'm thinking 'good grief,' you know, it's not even safe."

McElwain is not the only businessman who worries about the state of customer security as technology evolves. Joe Flannery, president of Weaver's Department Store, said that the fear of cyber theft became more apparent after Target's data system was breached

last year. He said that made him realize that businesses should continually be wary, because it was something that could happen to any of them.

"We can't be protected until the technology changes," Flannery said. "It's too easy today to get hacked, and too many companies are being hacked. Small businesses just need to be as attentive as possible."

Flannery said that credit card companies have been working on new technology that will help protect shoppers from potential breaches. One major change that credit card companies may implement soon is the switch from the magnetic strips on credit cards to metallic chips. According to the Bank of America, these chips will encrypt information and make it much harder for criminals to replicate. Flannery said the chips will also require that businesses and banks change the technology that they use in their check out terminals.

"Right off the bat, spending the money might feel frustrating, but I would say the cost would probably be insignificant enough, especially if it does cut down on credit fraud," Guffey said.

Flannery said he agrees that these information chips are worth the cost of the extra equipment. He believes that it is part of a necessary change to protect both shoppers and businesses.

"Banks have been so hesitant because they haven't wanted to pay extra for completely new technology, but it's an inevitable change," Flannery said. "We're too vulnerable now."