lunch line at an elementary school cafeteria.

Jun. 03, 2016

Apparently, the heist couldn't have been any simpler if it had been drawn up in the lunch line at an elementary school cafeteria.

In February, Bangladesh's central bank saw $81 million disappear out a virtual window. Now it's been revealed that, although the computer hackers used custom-made malware, they probably didn't need to work up a cyber sweat while pulling off their long-distance theft. The bank had no firewalls to defend against intruders and its computers were linked to global-financial networks through second-hand routers that cost $10.

"It's stunning that a major institution would leave itself so defenseless in this day and age when everyone should know that cyber criminals are waiting for you to let your guard down," says Gary S. Miliefsky, CEO of SnoopWall (www.snoopwall.com), a company that specializes in cyber security. Miliefsky has been active in the INFOSEC arena, as the Executive Producer of Cyber Defense Magazine and a regular contributor to Hakin9 Magazine.

But he says the episode can serve as a cautionary tale for other banks and any businesses that want to protect themselves against today's cyber versions of Bonnie and Clyde.

"Most companies have some vulnerability and it doesn't take a sophisticated attack to cause a security breach," Miliefsky says. "Often on the hackers' end of things, it just takes patience."

For example, he says, a cyber criminal can gain access by sending a company an email with an attachment called a Remote Access Trojan, or RAT, that looks like a

normal file. All it takes is for an unsuspecting employee to open that file and, voila,

like unlocking the front door, so employees should be made aware of the dangers and told what do about suspicious email.

- **Companies should routinely update their defenses.** Outdated technology and outdated security software make a company's computers vulnerable to attack. It's important that businesses periodically review their IT operations to make sure what worked last year still provides the needed security.
- **Consumers must take their own safety measures.** It would be nice to expect banks and retailers to protect consumer information, but the average person can't count on that. Miliefsky suggests consumers take personal security measures such as frequently changing passwords and deleting any phone apps they don't use. Many apps contain malware that can spy on you.

"Most people log onto the internet every day without much thought about how susceptible they are to being hacked," Miliefsky says. "It takes vigilance to protect yourself against cyber criminals who are working hard to figure their way around security measures."

Security • Small Business • Technology