Be Prepared: Cyber-Criminals Can Wreak Havoc

How simple modification to a school district's crime policy saved them $100,000

NOTE: Since this article addresses an open case with local police and Secret Service, the school district will not be identified.

A Wisconsin school district payroll clerk followed established security protocol in the procedures for bimonthly payroll processing. The file was created by the payroll system and downloaded to the district's designated computer. The district payroll clerk retrieved the file, and then verified the data. With all data confirmed, the clerk transmitted the file electronically to the district's bank for overnight processing. Early the next morning, a district employee called to ask if there was a delay in automatic deposits.

There was more than a delay. The payroll batch file had been "cyberstolen" and replaced with new names and accounts all over the country for more than twice the amount authorized. The payroll money was gone.

Discovery, Fear… and then Relief

The district business manager shared the story:

"As soon as we got the phone call that something was wrong, we called our bank. They called the police and started to unravel what had happened. Our immediate priority was paying our employees. Working with the bank, we wrote physical checks for our employees and then our district team got into our cars and we rode all over the area, depositing that cash to our employees' accounts.

Our second call was to our account executive at M3. Here's the relief part of this story. A few months earlier, he had recommended additions to our crime policy based on the trends M3 tracks, like cyber-crime. I'm a 'cheap' business manager, but the low cost of these riders made it easy to say yes. That was the smartest decision of my career. We added coverage for Computer Fraud and Funds Transfer — a low deductible and a $250,000 limit. It cost less than we could have imagined, and it was the best money I have ever spent. We knew we were covered."

The investigation included the bank, the district, the local police, the Secret Service, the insurance company, M3 and their claim consultants, and even a forensic engineering company who specializes in fraud. The bank's disaster plan across banking networks helped them recover almost $250,000. The new insurance has covered the rest. The forensic team has pinpointed when and how the breach occurred; the Secret Service is pursuing the perpetrators.

Is Your Data Protected?

Data privacy is a hot topic for every individual and business. Consider the sheer volume of intensely private data maintained in government and education systems. Complex cyber-protection hardware, software and processes guard that data and the systems that manage it. But computer fraud perpetrators go well beyond "hacking". Their goal is access to money, personally identifiable information, trade secrets or military information. These criminals "spear-phish" with wide-ranging, email-based fraud attempts. Individual emails seem to come from personally trusted sources. But when opened, the email triggers download of spyware that can enter protected systems and access secured data.

As global networks grow larger and larger, we all have increased risk for data breaches. Here are just a few of the data breaches at Wisconsin educational and government institutions over the last five years.

- **2007:** The Wisconsin Department of Veteran Affairs
- **2009:** City of Madison
- **2009:** Wisconsin Department of Corrections
- **2010:** University of Wisconsin at Madison
- **2011:** University of Wisconsin at Milwaukee ■

5 steps towards certainty in an uncertain world

1. Audit your internal processes for all financial/confidential data protection. What's the backup plan for your backup plan?

2. Pay close attention to hardware as well as software. If your security system server goes down, what happens? That's when you're the most vulnerable.

3. Create an actual disaster plan with your partners such as your bank and your payroll system. Make sure you are all on the same page.

4. Train your employees. Email provides the easiest access into a protected network. Define what kinds of emails are dangerous to open.

5. Check your crime coverage. Work with your insurance company to ensure your crime coverage is up to date. Do you have an adequate limit? Will it cover your payroll?

"Of course, we have protection in place — a system of firewalls, passwords and process checks. What we learned is that protection can fail. **The hackers are one step ahead."**

— School District Business Manager