



Being Unaware is More Costly than you Think

by Barry Thompson, BOL Guru

[Guru Bios](#)

Security regulations seem simple and straightforward until a problem emerges. Too often, bankers are unaware of all the responsibilities placed upon them by security regulations. They believe that if they conduct annual security training and report annually to the Board of Directors, their obligations have been met. While this might pass regulatory inspection during examinations, the bank still might find itself negligent in an actual lawsuit.

The following are examples of actual cases that have resulted in negative publicity, turnover in staff, and expenses that exceed insurance coverage:

1. A staff member's family was taken hostage at home while the staff member was forced to open the bank branch.
2. A customer entered a branch only to discover that the teller and two other customers had been shot and killed. The teller was working alone.
3. A robber attacked a customer who fought him for his \$20 withdrawal from the ATM. The robber killed the customer.
4. During a robbery, a robber threatened a staff member's life with a lethal weapon. After the robbery, the bank refused to provide counseling for the staff member.

When one of these types of security cases transpires, management finds itself in a no-win situation. Any attorney who is going to sue a financial institution will hire an expert consultant familiar with the standards of the industry and the regulations the bank didn't fully understand. The bank will then receive a subpoena to produce evidence of its security program, policies and procedures, and the training materials used to educate staff. One institution that was sued commented that they could have filled a 12' x 12' room with the material subpoenaed by the attorney, and the attorney, accompanied by the expert consultant, will interview anyone even remotely involved with the case.

Eventually, these cases were settled outside of the courtroom. The consultants involved signed a nondisclosure agreement stating they'd never reveal the final settlement agreement, and the insurance companies refuse to reveal how much they paid to settle the lawsuits (because they don't want this to become common knowledge in the industry). However, the damage had been done. Without a doubt, negative publicity in the media has caused harm to these institutions' images.

If, however, the banks involved in the cases above had been aware of industry standards and regulations, no staff member would have been allowed to open a branch by himself/herself, proper lighting would have been installed around bank property, and psychological counseling would have been offered to staff immediately after the robbery. Knowing the standards of the industry could have saved these banks time, money, and negative publicity.

How can your institution avoid these lawsuits, or at least reduce the potential payout, which could potentially

range in the millions?

1. Make sure at least one member of the senior management team has attended security training involving the duties and responsibilities of the security officer.
2. Send your internal auditor and compliance officer for security training updates periodically.
3. Send your security officer for annual training.

Fraud perpetrated against financial institutions amounts to more than just a game of cops and robbers. Financial institutions everywhere are losing money to cyber crime, Nigerian scams, and frauds masterminded by organized gangs, and this year, the newest frauds are being conducted against business accounts via ACH or direct attacks. Is your financial institution prepared for what lies ahead?

First published on BankersOnline.com 2/15/10

Original Article Located at http://www.bankersonline.com/security/guru2010/thompson_article021510.html
Copyright, 2000-2014, Bankers Online. All rights reserved.
This information was printed from the BankersOnline.com web site located at <http://www.bankersonline.com>