WORK FROM HOME SCAMS AND COMPUTER FRAUD

Propel Insurance
By Charlie Morriss

Somewhere, in a neighborhood near your office, a 24-year-old is looking for work. Maybe he posts his resume on Monster.com or Craigslist or Careerbuilder.com. He'd rather have a full-time job, but he has been out of work for months, and is open to any opportunity, including working from home.

He gets an offer from Best Inc., a "software developer" supposedly based in Australia. They arrange a telephone interview, and offer him a work-from-home position as a Research Assistant. His compensation: commission on software fees, 5% of all fees collected from clients in his assigned territory.

His first assignment: a market study of the number of doctors practicing in a five-county region. To his surprise, even before he completes his assignment, his first commission the next Saturday arrives in the form of an electronic payment from a local medical center. As instructed, he forwards the payment, minus his 5% fee, to the "software developers" in the Ukraine.

This 24-year-old is not a Research Assistant, as he believes himself to be. He is a mule. Best Inc. is a criminal enterprise that has hacked the medical center's computers and sent the funds from their bank using stolen passwords and without authorization.

Not only that, but there are 100 other mules in the state with nearly identical experiences that made similar transfers to the Ukraine. They all occur in the same weekend, and are not discovered until the following Monday. The amounts were all too small to trigger the attention of the medical center's bank. The money - nearly $1,000,000 - is gone.

Will the bank restore the medical center's funds? Doubtful. The bank itself did not suffer a breach of security, the medical center did. The bank has met its contractual obligations to its customers, and its procedures where consistent with banking industry standards.

These work-from-home scams, and other high profile hacker attacks like the on suffered recently by Target Corporation, highlight the need for two types of insurance: Computer Fraud Insurance and Cyber/Data Breach Insurance. Computer Fraud Insurance covers the theft of money

through the use of computers, while Cyber/Data Breach Insurance covers the theft of information such as credit card numbers, social security numbers, or other Personally Identifiable Information ("PII").

Computer Fraud coverage is simple in concept. If you have lost $500,000 to a hacker who drains your bank account, the insurance pays you $500,000 (minus the deductible). It is an insurance product that has been available for decades, but also one that many companies overlook or choose not to purchase.

Cyber/Data Breach Insurance is more complicated. If 100,000 medical records or credit card numbers are released, what are the costs that can be insured? First, there may be lawsuits alleging negligence in how the data was stored or how the breach was handled after it was discovered. Second, the victims must be notified in accordance with state laws (47 states have them). Finally, legal fees, forensic services, public relation firms, call centers, and data restoration costs can all be included in the insurance coverage.

Every business has these exposures. They should certainly be addressed proactively by IT professionals and managers who design secure systems and information storage policies, but insurance is also available to protect the bottom line if the event your business falls victim to this growing threat.

The question to ask is this: If your business suffers a hacker attack, would you rather have a response team put together and paid for by an insurance company, ready to respond with one phone call, or would you rather track-down and negotiate with these service providers in the critical hours after you have discover a breach?