Butwin Insurance Group

Founded 1925

Understanding Deceptive Funds Transfers, Social Engineering and Cyber Crime: Exposures and Solutions

You receive an e-mail which appears to be from an executive of the firm instructing you to wire funds to a specified address.

You receive an e-mail or call which appears to be from a vendor instructing you to change its banking information.

Social engineering, a term for the manipulation of humans into performing acts or divulging confidential information, is not a new concept. A social engineer is nothing more than a con man who uses technology to swindle people and manipulate them into disclosing passwords or bank information or granting access to their computer. Understanding how these social engineers work and the schemes they employ is key to implementing successful internal controls which minimize the risk of loss.

There are at least seven potential scenarios for deceptive-funds transfers:

1. The fraudster, through emails, telephone calls or both, posing as a company executive, vendors or customers, convinces an employee to transfer funds
2. The hack and transfer are enabled by employee negligence
3. The transfer is effected entirely by a hacker independently penetrating a computer system, and making the transfer
4. The fraudster convinces an employee to reveal credentials, enters the network by using them, and then transfers funds
5. The fraudster gets an employee to open an attachment or click on a link, thereby allowing the network to be penetrated, and allowing the transfer of funds
6. An employee enters data believed to be accurate which in fact is fraudulent
7. A rogue employee makes an improper transfer or enters fraudulent data

Often Insurance is Not The Best Risk Management Solution. We Recommend That Everyone Implement Loss Control Procedures and Training.

The growing use of technology-enabled fraud is evolving faster than the courts or insurance carriers can react to them. Crime Insurance was designed to cover an employee stealing from the firm. Cyber Insurance was designed (in addition to other exposures) to protect against an outsider hacking into your computers. **Neither policy was designed to cover an employee's conscious decision to intentionally release information or funds, even if induced through fraud or deceit.** Insurance carriers have begun to roll out coverages to protect against these exposures. There are still many problems remaining:

- The carriers themselves are not sure what all the exposures are and how to properly cover them.
- The coverages being offered are completely different from carrier to carrier. They are all very limited on their own and compared to each other.
- The exposures are spread out over: Messages from Trustworthy Sources, Phishing Schemes, Baiting Scenarios, Impersonating Superiors, Computer Fraud and Funds Transfer Fraud. There is no one product to protect against all of these exposures. There is no sure and tested group of products to fully protect against all of these.
- Due to the newness of this fraud, courts have not yet established which coverages are actually responsible to respond to these losses.

Often Insurance is not the best Risk Management solution. We recommend that everyone implement at least the following Loss Control Procedures and Training:

- **NEVER** add new or edit existing wire transfer instructions without making an outgoing phone call confirming the instructions are from the requestor.
- **NEVER** open an attachment, download a file, provide or confirm information, etc. from any person via an e-mail even if you recognize their name. **FIRST HIT "REPLY" and CAREFULLY CONFIRM that the e-mail address showing in the reply e-mail address confirms WITHOUT A DOUBT that this is the person they say they are.**

"2 A.M. is a lousy time to find out you chose the wrong insurance broker"

60 Cutter Mill Road, suite 414, Great Neck NY, 11021 · 516-466-4200 · www.butwin.com · info@butwin.com