MORETON & COMPANY

CATCH SOCIAL ENGINEERING FRAUD - BEFORE IT HAPPENS

It seems that every day criminals are coming up with new, more sophisticated ways to con individuals and businesses out of their money. The most recent trend is a scam that has become known as Social Engineering, or corporate deception fraud.

WHAT IS SOCIAL ENGINEERING?

It is a fraudulent request for a wire transfer, typically made through email or phone call, where the requester is impersonating an individual such as an employee, a client, or a vendor. The request is usually targeted to individuals with access to banking information or payment authority, but not always.

Criminals have become very sophisticated in their approach. They can impersonate an email address that appears to come from within the company, or familiar vendor or client. They have been known to phish employees within the company for access to information that might help their scam and may even develop relationships with employees to gain their trust and manipulate targets.

> "Over 100,000 people are affected by social engineering attacks each day"

WHO HAS BEEN AFFECTED?

It has been reported that over 100,000 people are affected by social engineering attacks each day [1]. Both small and large businesses are targeted, with 41% of large business, 25% of mid size business, and 34% of small businesses being affected in 2015. 1 in 2 small businesses and 5 in 6 large businesses have been targeted in the same time period [2].

Historically, these Social Engineering schemes have not been appropriately addressed by management, professional, and cyber liability insurance policies, which are constantly evolving due to changes in technology and other exposures. This is because a third party is not hacking in to the network and taking funds but rather the company's employees are willfully departing or sending the money (via deceptive practices of a third party). Many companies don't even know they have fallen victim to Social Engineering until it is too late and funds have been wired to an account that is immediately emptied, leaving the company with no way to recover the funds.

Insurance carriers are now addressing this exposure on their crime polices through a Social Engineering endorsement. Many carriers offer small sub-limits for little to no premium, and higher limits may be available subject to proper controls in place for verification of wire payment requests.

BEST WAYS TO ADDRESS SOCIAL ENGINEERING FRAUD

- **Work** with your insurance broker to ensure you are appropriately covered to provide a financial backstop when social engineering fraud does occur.
- **Educate** employees about social engineering scams and limiting transfer authority to specific employees.
- **Enforce** an independent call back verification of all transfer requests to ensure validity of such requests.
- **Require** next-level supervisor sign-off of any changes to vendor and client payment information.
- **Never allow** the urgency of a message influence your careful assessment of a wire transfer request.

[1] Hilard Heintze The Front Line Report
[2] Symantic Internet Security Threat Report 20