FRAUD ADVISORY: SOCIAL ENGINEERING AND HOW TO PROTECT YOURSELF

Social engineering, whale phishing and e-theft are buzz words for the latest form of fraud, perpetrated by those who lie, cheat and scam their way past security controls in an attempt to part an organization from its money or securities.

HOW IT WORKS
Fraudsters send communications to an employee (most often via email, telephone or a combination of the two), which are doctored to appear as if they are sent by a senior officer of the company or by one of its customers or vendors. Instructing the employee to wire funds to a particular bank account, the communication stresses the need for absolute secrecy, perhaps citing the fact that the fund transfer is related to a pending IPO or other confidential transaction that requires normal authentication procedures be bypassed, while also citing urgency. Some schemes are highly complex and can actually result in the undetected rerouting of phone calls or email domain changes.

For those instructions purportedly coming from a vendor or customer, the schemes can be embroidered by informing the employee that they have changed banks and require the company to provide new wire instructions for all future payments.

PREVENTION
Implement and require strict adherence to such basic loss mitigation procedures as:
- A call-back procedure to the individual that purportedly sent the instruction
- Prearranged passcodes
- Maintaining a list of individuals in the organization and in the customer’s or vendor’s organization authorized to initiate a fund transfer
- Confirmation via a phone call or email to authorized person at a customer’s or vendor’s that they have changed banks or any account numbers

The above procedures are effective in preventing many losses. Unfortunately, a surprising number of companies have not adopted even the simplest controls to avoid falling prey to these schemes.
RISK TRANSFER

While fidelity coverage is a staple of a comprehensive risk transfer program, the overwhelming majority of crime policies do not cover these losses unless the insured's own employee is involved in the scheme. Forms used by several leading markets arguably contain an element of coverage for these loss scenarios when the instruction purportedly comes from an employee of the insured. The cover, however, is limited to instructions purportedly coming from an employee and does not include those purporting to come from insured's clients or vendors, which has also been a frequently used scheme.

In response to this loss trend, one leading carrier has now launched their new Social Engineering Fraud Endorsement that will provide coverage for a range of social engineering fraud losses, including:

- Vendor or supplier impersonation
- Executive impersonation
- Client impersonation

Having reviewed the endorsement, we can confirm that:

1. The endorsement employs broad all-risk language; i.e., it provides coverage for all types of social engineering frauds.
2. Limits of liability up to $250,000 are available, although higher limit options, in some cases up to full policy limit, will be considered for risks that have appropriate controls in place. All limits greater than $1,000,000 will require a minimum retention of $250,000.
3. A supplemental application form is required for all social engineering fraud coverage requests.

Note that the application needed to purchase this coverage is robust. Unknown at this time is the availability of coverage for applications whose responses are less than stellar and whether those having excellent controls already in place feel the need to purchase the coverage. In the end, however, it is fair to state even the best internal controls do not guarantee prevention of some of these highly complex schemes.

CONTACT

Stephen Leggett
Executive Vice President
Willis Americas Administration, Inc.
FINEX North America
stephen.leggett@willis.com

Executive Risks Alerts and Newsletters provide a general overview and discussion on a wide range of topics. They are not intended, and should not be used, as a substitute for legal advise in any specific situation.

Willis North America Inc.
Brookfield Place
200 Liberty Street, 7th Floor
New York, New York 10281-1003, United States
Tel: +1 212 915 8888
www.willis.com

50680/11/14