

## BLOGS

Cyber Insurance

# Social Engineering Cyber Coverage: Protecting Your Company from the Human Factor

Remember those spam emails from Nigerian royal family members needing to transfer millions of dollars out of Nigeria, requesting the recipients provide banking and personal information to “hold” the funds or otherwise front money to the fraudster to pay taxes and fees? While most people have (hopefully) wised up to that scheme, a more insidious and devastating fraud has taken hold in the corporate world – the “social engineering” scheme.

“Social engineering” schemes are shades of the Nigerian letter scams, except the fraudster pretends to be someone affiliated with your company, such as a contractor or vendor. The emails are convincing even to sophisticated employees, often instructing the recipient to follow “corporate procedures” to complete the money transfer.

Typically, this is how the scheme works:

- (i) Your employee receives a phishing email from a spoofed address where the fraudster pretends to be affiliated with your company and requests a transfer of an (often substantial) amount of money;
- (ii) Your spoofed employee follows in-house protocols with respect to the requested transfer, sometimes even getting approval from more senior level management;
- (iii) Your employee makes the transfer to the fraudster’s account; and
- (iv) Your company discovers the fraud only after the transfer.

Many companies are shocked to find only after the fact that their insurance carriers do not cover these losses. Unfortunately, not having appropriate cyber coverage can be a devastating mistake. The National Cyber Security Alliance found that as much as 60 percent of hacked small and medium-sized businesses go out of business within six months after being hit with a cyber-attack.

Businesses can greatly reduce the threat by mitigating cyber risks through managerial and technical processes, including implementing security measures such as firewalls, duo layer computer access, limiting employee access to sensitive data information, analysis of third party vendor’s security procedures, and regular and thorough training of employees. However, even the best measurers cannot

## Related People

### Alexander (Alex) T. Brown

Partner

Kansas City

816.460.5629

[alexander.brown@lathropgpm.com](mailto:alexander.brown@lathropgpm.com)

fully neutralize cyber threats. Businesses remain vulnerable because of the “human factor” associated with these schemes; a skilled fraudster executes a social engineering scheme with the (unwitting) help of an innocent employee.

Recent court decisions highlight the importance of closely reviewing cyber policies to ensure that “social engineering” scams are fully covered. In *Apache Corporation v. Great American Insurance Company*, 662 F. App’x 252 (5th Cir. 2016)[1], for example, the court held that the policyholder was not covered for social engineering attack despite having “computer fraud” coverage providing coverage for “loss of ... money ... resulting **directly from** the use of any computer to fraudulently cause a transfer of that property....” The Apache employee received a spoofed email with a signed letter on the vendor’s letterhead, instructing the employee to change the vendor’s account information and submit future payments to the new (fraudulent) account. The employee even called the telephone number provided on the (forged) letterhead and verified the request, while still another employee approved the transaction. Apache thereafter submitted payments to the new account. The Fifth Circuit held that the \$2.4 million loss was not covered because the computer use was not the **direct result** of the loss, but “merely incidental” to the fraud.

This case highlights how critical it is to companies to transfer the risk of all cyber-attacks through comprehensive cyber coverage, particularly to cover risks that cannot be fully mitigated by security measures because of the “human factor.” For this reason, it is important to review policy terms to assess the scope of coverage with your broker *before* your company is attacked.

[1] <http://www.ca5.uscourts.gov/opinions/unpub/15/15-20499.0.pdf>