KAUFMAN | DOLOWICH

Mansfield Rule Certified 2022-2023

4 Tips For Companies To Shield Against Phishing Scams, *Law360, ft. Stefan Dandelles*

Stefan R. Dandelles, partner in the Kaufman Dolowich & Voluck Chicago office, was quoted in a *Law360 article written by Jeff Sistrunk.*

Law360 (April 20, 2018, 8:20 PM EDT) — A recent report by specialty insurer Beazley detailing the prevalence of email-based "phishing" theft schemes illustrates the need for companies to build up robust defenses including employee education, preventative policies and insurance tailored to such risks, experts say.

Scope Out Social Engineering Coverage

"Some insurers are asking more rigorous questions regarding funds transfer policies and procedures," explained Kaufman Dolowich Voluck LLP managing partner Stefan Dandelles. "In the application, if an insured wants social engineering coverage, there is often a separate page or rider to the application that is narrowly tailored to that coverage, and it will ask, among other things, whether the prospective policyholder has any verification procedures in place."

"Brokers know which insurers they can go to for social engineering coverage with a lower threshold, perhaps without a separate application or conditions precedent in the policy," Dandelles said.

According to Dandelles, some insurers are offering different retentions or limits depending on how many conditions a prospective policyholder is willing to fulfill.

"For instance, [an insurer] may say if a prospective policyholder doesn't want the extra application or conditions precedent, it will only get a limit of 'X' or a high retention amount," he said. "On the other hand, if the policyholder agrees to a full application and a verification procedure built into the policy, the insurer may offer higher limits or a lower retention."

Don't Use Insurance as a Crutch

"I don't think anyone wants the moral hazard associated with companies looking at insurance as an easy backstop and saying, 'I don't need a verification process because I will get coverage if I get duped,'" Dandelles said. "A company should want to implement best practices to avoid having to turn to their insurance coverage at all."

Dandelles noted that a company may incur a number of "soft costs" due to a social engineering incident that won't be picked up by insurance, including loss of reputation, decline in employee productivity and payments to outside lawyers, IT vendors and other consultants.

"Every policyholder should be keenly aware of these other exposures and implement training and proper protocols to prevent these incidents," he said.

If policyholders fail to maintain adequate preventative measures and insurers end up paying out more social engineering losses as a result, the availability of specialized coverage would decline and premiums would rise, according to Dandelles.

But on the other hand, he said, if policyholders "take appropriate and necessary steps to avoid or at least limit these losses, and the insurance market becomes more comfortable that the companies they are insuring are doing the right thing, policyholders will likely see a positive impact on what's available to them and at what cost."