Social Engineering: The Human Risk

There's a pervasive risk that's growing in scope and complexity that could well level a significant blow to your staffing firm. Social engineering combines the reach of technology with the art of manipulation, and involves everything from a request for assistance by an unknown entity in a foreign country to an urgent call from a friend or relative requesting money to get out of trouble.

The term "social engineering" belies the severity of the risks such attacks bring to companies. Every business needs to understand and address social engineering because every business is vulnerable – even ours. It happened at World Wide just a month ago that a fraudulent request for a wire transfer came in. Because we had procedures in place, not only in-house but also with the bank, the attempted theft was thwarted.

And while wire fraud is just one method of social engineering, the FBI reports a 270% increase in identified victims of such attacks in 2015, costing losses over $747 million.

Are you and your clients prepared?

For staffing firms, the problem is amplified with employees working onsite at client locations. While many staffing firms have tight controls around their own approvals and expense requests, just as many clients may not.

Also, not all clients are expecting temporary workers to follow the same procedures when it comes to responding to requests. How does the employee verify that the charge being requested by your employee in accounting is actually coming from that employee.

Now knowing such procedure could mean your employees may unwittingly open the door for thieves, particularly if clients are not ensuring that the temporary staff are following the same guidelines they expect regular staff to follow. The cost of such an oversight could hit not only your client, but your own staffing firm.

Even insurance, while a necessary part in protecting your business, it isn't the only solution you should have in place. Develop a social engineering prevention process. Teach staff and employees that process, and talk with your clients about the risk. Verify that your clients have a social engineering protection plan, and find out what they are and how they are being applied to temporary and contract workers. Are they addressing the risk and if not, have they agreed that your employee won't be responsible for such losses?

Knowing what your responsibilities are and how to mitigate the risks can further ensure that your business and your client's business are doing as much as possible to protect against social engineering theft.

We at World Wide have been part of the staffing insurance industry for over 50 years. Our deep level of claims experience gives us a comprehensive understanding of the risks your company faces. Talk to us. We're here to help you and your broker understand social engineering risks and how to mitigate them.

If you are not sure if your insurance portfolio includes coverage for a social engineering loss and you need guidance in putting together a social engineering dialogue to address with your clients…Contact us