TAKING STOCK

A PERIODIC EXAMINATION OF KEY ISSUES AND TRENDS FROM MARSH'S RETAIL/WHOLESALE PRACTICE

THIEVES GAINING ENTRY THROUGH SOCIAL ENGINEERING

If you think your company's money is safe because your software is up to date, you screen the people you do business with, and you limit access to wire transfers, consider the following:

- An attacker pretended to be the CEO of a company subsidiary and tricked an employee into transferring more than $40 million dollars.
- A scrap metal processor wired $100,000 to an overseas vendor to pay for titanium shavings, but the payment instead went to a thief who falsified the transfer instructions.

These are examples of robbery by way of social engineering — where fraudsters rely on words and positioning, not guns, to steal.

A SOPHISTICATED SCAM

Social engineering is also known as impersonation fraud. Would-be thieves learn as much as they can about a company, its people, and its processes through publicly available information: annual reports, corporate blog content, newspaper articles, and even investor calls. They get a feel for the way CEOs, CFOs, and others speak and act. After conducting research, they combine what they learned — and sometimes computer hacking — with their ability to be persuasive to gain access to a company's confidential data. In short, the act of social engineering is simply making communications appear to come from a trustworthy source.

Earlier this year, the FBI said it expects to see a dramatic increase in social engineering crime, what it calls "business email compromise." The agency said there was a 1,300% increase in identified exposed losses between January 2015 and June 2016, to a global total of more than $3 billion.

Retailers and wholesalers are particularly vulnerable to social engineering because of their extensive relationships with suppliers and vendors. A typical scam might run like this: The thief pretends to be a known vendor and reaches out to accounts payable, advising of a change in account information. Since the employee believes the request is coming from the real vendor, they make the payment to the new account. Result: The funds are gone and the true vendor has not been paid.

It might seem that such a brazen crime would be difficult to pull off, but that's what the research ahead of time is for. The crook that uses social engineering as a weapon may create an email address that looks just like the real thing. Using almost-right information convinces unsuspecting employees to provide access to the fraudster.

Keep in mind that money may not be the desired end-goal — a loss of data can be just as damaging as a direct financial hit. For example, companies of various sizes have been victims of scams that ask employees to submit their W2s to a digital mailbox for "something having to do with the IRS." The email may even appear to come from your human resources department with all the expected markings and logos. In one case, the fraudster was able to retrieve all 20,000 employee records before the scam was detected.

MARSH

IMPROVING ORGANIZATIONAL AWARENESS AND MITIGATING THE RISKS

A social engineering attack can be costly for both your bottom line and your reputation. And it can be months before a problem is even discovered, much less remediated. Consider what could happen if criminals are able to obtain and manipulate valuable data.

For some, a security audit and a detailed overhaul may be called for. But there are also steps you can take immediately to help strengthen your defenses, including:

- Establish and require training and continuing education courses for employees on safe and proper use of internet functions, including how to verify email addresses, domains, and the like.
- Set up a verification procedure for employees with questions about the veracity of a call or email.
- Try phishing your own staff to get a pulse check for how susceptible people are, and where you may need to build more awareness. There is software designed for doing this, which your IT department should have more information about.
- Enforce effective password management.
- Understand what your insurance policies cover. For example, if you have both a cyber policy and a crime policy, how might they interact in the event of a social engineering loss?

The big takeaway is to remember that every business is a potential victim of social engineering. By creating a culture of awareness while implementing appropriate risk management and insurance strategies, you can help your organization and employees recognize and mitigate the potential impact of this kind of theft.

This briefing was prepared by Marsh's Retail/Wholesale Practice, in conjunction with Marsh's FINPRO Practice.

For more information about social engineering and other insurance solutions, visit marsh.com, contact your Marsh representative, or contact:

MAC NADEL
Retail/Wholesale, Food & Beverage Practice Leader
+1 203 229 6674
mac.d.nadel@marsh.com

Marsh is one of the Marsh & McLennan Companies, together with Guy Carpenter, Mercer, and Oliver Wyman.

This document and any recommendations, analysis, or advice provided by Marsh (collectively, the "Marsh Analysis") are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, tax, accounting, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. Marsh makes no representation or warranty concerning the application of policy wording or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage. Although Marsh may provide advice and recommendations, all decisions regarding the amount, type or terms of coverage are the ultimate responsibility of the insurance purchaser, who must decide on the specific coverage that is appropriate to its particular circumstances and financial position.

Copyright © 2016 Marsh LLC. All rights reserved. MA16-14009 20166