ceocfointerviews.com

Issue: March 21, 2016
The Most Powerful Name in Corporate News

Security Awareness Training for Enterprises to Manage their IT Security, Change Employee Behaviors and Prevent Spear Phishing and Ransomware Attacks

Stu Sjouwerman
(pronounced "shower-man")
CEO & Founder
KnowBe4, Inc.

CEOCFO: ***Mr. Sjouwerman, what is the concept behind KnowBe4?***
Mr. Sjouwerman: The concept is new-school security awareness training, as opposed to old school where you do this once a year which does not work. What we do is a three step process. It is really simple. You send a simulated phishing attack to all employees, which is your base line, and the percentage of how many people clicked. That is your phish prone percentage. Second, you now announce that to all employees and say that we have a problem that needs to be fixed and train everyone, which is online, on demand, engaging training through the browser whenever they have time. Step three is continuing with frequent simulated phishing attacks year-round to keep employees on their toes with security top of mind.

CEOCFO: ***Are you surprised at how many people still do not understand that basic concept of not clicking on a suspicious link?***
Mr. Sjouwerman: They simply have not yet been enlightened about the dangers of the internet.

CEOCFO: ***In 2016, you feel that is the case?***
Mr. Sjouwerman: That is still the case.

CEOCFO: ***What types of information would hackers be looking for at a school, for example?***
Mr. Sjouwerman: For example, they are interested in records that allow them to steal someone's identity. Monday morning, my controller caught an email supposedly from me, which it was not. It said "Urgent request, I need W2s of all employees in a PDF, please email this to me." If you know what is in a W2, it is name, address and everything. They could file a tax return if they wanted to. Those are the kind of records they are looking for so that they can either use it or sell it.

CEOCFO: ***How do you get through to people that they have to be vigilant?***
Mr. Sjouwerman: Truly, the first thing is that you explain to them *and show them* the consequences and potential repercussions of opening an infected attachment. You need to make it real to them that their whole computer might get encrypted, and they may need to pay $500 to get their files back. What that actually means and how many hundreds of hours you will have to go through, until it happens to you, you do not really know what it is like. Awareness training does that.

CEOCFO: ***Who is your typical customer?***
Mr. Sjouwerman: It varies. 25% of our customers are banks and credit unions for obvious reasons. We do have school districts as customers, and generally speaking, they are not the highest sophisticated in IT defenses because that is not their mandate. They know that they are vulnerable and that is why they wonder what the best investment is. The best Return on Investment for School Districts is to see if they can mitigate this problem. That is why they call us.

CEOCFO: ***Are financial institutions remiss is requiring vigilance from their employees?***
Mr. Sjouwerman: There is a difference between security and compliance. From a compliance perspective, they have done this for years. If you are a financial institution, you have your GLBA and FFIEC kind of industry regulations. You have to do security awareness training as part of what they call controls, meaning the things you need to do to be safe. If you grab all employees and herd them in the break room for 20 minutes, you keep them awake with coffee and donuts and you expose them to "Death by PowerPoint" awareness training, then you can check the compliance checkbox and say yes, you are compliant. They also know that two weeks later, people are as click-happy as they were before, so that does not work. That is why they come to us, because our program, the way we have put it together actually gets a dramatic decrease in click-rate.

CEOCFO: ***Are you reaching out to clients on an individual basis or are you working through partners?***
Mr. Sjouwerman: We are a strictly B2B outfit. In this lifecycle stage of our company, about 80% of our sales are directly to organizations but we do have channel partners and that means people are reselling our product. There are managed service providers, MSPs who use this for their customers. We have a few OEM partners who have taken our platform and branded it with their own logo and they are selling this to their own customers.

CEOCFO: ***How do you reach out?***
Mr. Sjouwerman: By far, our most successful marketing strategy is very old fashioned, which is a weekly newsletter that goes to a large amount of the people that we sell to. We sell to IT people in the trenches, the IT administrator, network administrator, director of IT and the people that have as their goal in life to keep the network up and running. They understand that employees are the low hanging fruits for hackers. Employees are the weakest link in their network, so they are very motivated to get these employees trained.

CEOCFO: ***Why are men more prone to clicking than women?***
Mr. Sjouwerman: That is a good question. We do not know. We just know that this is the case. The numbers tell the story.

"The best practice is at the very least, do one simulated phishing attack per month." - Stu Sjouwerman

CEOCFO: ***How do you make training engaging so that people are going to pay attention?***
Mr. Sjouwerman: That is done by making sure that with any concepts you train people on, you want to make sure there is immediate understanding of a new term you are introducing. For instance, everyone knows what spam is, but not many people are aware of what phishing is, so we immediately define that and make it very clear. Almost nobody knows what spear phishing is, so we go into that in great detail. We make it interactive. We do little comprehension tests on a regular basis in the training so that they get feedback if they got it or not. We do our utmost to make this extremely accessible for anyone.

CEOCFO: ***Do you find the same culprits?***
Mr. Sjouwerman: Yes you do, but the best practice is not to wait that long. The best practice is at the very least, do one simulated phishing attack per month. You quickly flush out the repeat clickers and you can put those through a remedial training online. You can set that on automatic. Someone clicks and a minute later, they see and email in their inbox that they missed on a phishing test and to please step through this training.

CEOCFO: ***What has changed as your product has been available? What have you learned since the beginning of the Knowbe4 process?***
Mr. Sjouwerman: We have learned that the concept works. My background is IT security software, so we were building firewalls and antispyware and antivirus intrusion detection. We continued to see in my last company that people were infecting their machines. Social engineering is actually what the biggest problem is because the bad guys manipulate the employees into giving that bad guy access to the network. My main and most happy discovery was when we looked at 300,000 employees over many hundreds of customers and we took at twelve-month analysis. We found that it started at 16% and after twelve months, it was just over 1% of people clicking. We were very encouraged that the program actually delivers.

CEOCFO: ***How big a factor is cost for your customers? Do companies understand the value vs. cost?***
Mr. Sjouwerman: They do. If you look at the market, there are a few organizations that do somewhat similar things that we do but they focus on large enterprise. Their pricing is commensurate. We focused on small and medium business in the beginning but now we also have enterprise-size customers because our feature set is now enterprise level but our pricing is extremely affordable. Price has almost never been an actual problem simply because we want this to be affordable for everyone. There are a couple hundred thousand organizations nationwide that needs this and we wanted pricing to not be an issue. I prefer to have thousands of small customers rather than a few big ones.

CEOCFO: ***What is next for KnowBe4?***
Mr. Sjouwerman: We are going to do an IPO, however that might still be a few years down the road but we want to continue to grow. Just this morning, I received and email that we had been accepted for the INC. 5000 list, meaning our submission was accepted.

CEOCFO: ***Why should everyone be paying attention to KnowBe4 today?***
Mr. Sjouwerman: If you analyze malware and phishing attempts, only 3% of attacks are focusing on some kind of software vulnerability. 97% of the phishing attacks are focused on the human, so any organization that has their employees on the internet has a major vulnerability that needs to be addressed. This is an ongoing problem that needs to be managed. As you may have noticed, I am not using the word "solution." We do not sell a solution, we sell a subscription to manage and ongoing problem. As long as the internet is still in beta--which it is-- you will continue to have this problem. Any organization that wants to keep their money in the bank should have a thorough look at what we call "new-school" security awareness training.

Interview conducted by: Lynn Fosse, Senior Editor, CEOCFO Magazine

---

KnowBe4, Inc.

For more information visit:
www.KnowBe4.com

Contact:
Stu Sjouwerman
727-493-5296
stus@KnowBe4.com