ICMI 2019
Stridepoint

Todd Snapp, President and Nathan Caldwell, Security Awareness Evangelist, Stridepoint. Our primary goal is to secure contact centers… both the agents and the environment. When we're brought in, it's either that there is a concern that agents are giving out more information than they should, revealing private information about their customers, or that they have already experienced a breach and need to take action to resolve it. Once we are involved, one of our main purposes is to assess the risk and determine where the weaknesses are in a company's security. We do tests and provide training; it is often compliance-oriented but also could be behavioral—helping a company's employees defend themselves against fraud or deception.

Our impetus is to create a culture of security—developing a mindset to defend against security threats. A lot of people are now acknowledging that security needs to be both part of a business plan and an integral part of their practices. We often work with technology experts who are responsible for implementation to show them how to prove the value and position it so that leadership wants to adopt it.

We use the term "social engineering". This term refers to con artistry. It is defined as 'I'm going to hack a company, not through the servers or the network, but through its people.' That's why it's so important in the contact center because their people are their primary interface and might be susceptible to attempts to get information or click on links that would enable hackers to infiltrate the organization. It is usually based on deception, such as pretending to be a customer, an employee of the company or even law enforcement. We go in as "ethical hackers" to determine vulnerabilities.

In the tests we've been doing for 15 years, on average, more than 30% of calls or emails coming in compromise an account. More than 90% of breaches happen because of the actions of people as opposed to through computers. Security training needs to be a part of onboarding process and a perpetual part of their culture. Contact centers have traditionally been totally focused on training to improve customer service. This leads agents to believe they must be helpful at all times, so when they try to lead customers through a stated issue, they don't realize they are putting themselves and their company at risk by often divulging too much information to someone with bad intentions. Of course, they must strike a balance - providing a positive customer experience is paramount, but it must be done in such a way that security is maintained.

Awareness of the need for security in the contact center is growing because of highly publicized breaches, particularly in some household name companies that have approached us. But security is something that a business needs to be prepared to address ahead of time, not after a breach has already taken place. Breaches don't only happen in big name organizations and can be fatal to smaller companies who often have a false sense of being immune. Sometimes, it's small companies that are vendors to larger businesses are the cause of breaches due to weak security. In some cases,

the big organizations are now requiring the contact centers of their business partners to be protected. In addition to contact centers, we are also brought into determine security in other departments, including IT which is sometimes the most vulnerable area. We are also instituting a program to help companies engage customers to learn how to better protect themselves. Social engineering threats include everything from malicious personal information gatherers to child predators to industrial spies and even gamers trying to access other players online wallets. Snapp elaborated further:

Why do you consider it vital for businesses to make security, compliance and awareness as engaging as possible for their employees?

Because of compliance, HR and security risks, many employees are hit with a barrage of training every year. Historically, this is a necessary evil that employees power through to meet requirements. (Check a box) Some of these topics, though, represent the only way that some companies prepare their people to protect against serious threats.

When it comes to security, the material has to be presented in such a way that people will recognize the value and pay enough attention to really absorb the information. Not only do they need to be engaged enough to learn what is being taught, but also to remember it when it is needed.

Can you shed light on how you work one-on-one with clients to develop custom content?

With some clients, the presentation of security and compliance training needs to be customized to match the unique policies and threats of their industry. In other cases, just the personalization of the material to match the terminology and culture of the organization goes a long way to engage the audience and demonstrate the value of the material to the specific audience.

What are some of the most serious social engineering threats to sensitive data that businesses encounter?

Most companies recognize the reality of deception and “con-artistry” as a threat to their security, but few realize the damage that has been done by fraudulent phone calls and emails. Most of the “front page news” security breaches of the last 10 years came from social engineering breaches. Customer accounts have been compromised, giant databases of personal information have been lost and companies have been devastated because their front-line employees were ill-equipped to defend against a devious phone call or message.

How do you help call centers focus on what you term “The Human Side of Security?”

Contact centers play a vital role in the both the customer service and security posture of a business. We have worked with countless contact centers where the organization has spent millions of dollars and thousands of hours protecting their network and systems (and rightfully so) but are stymied when it comes to building the “human firewall” with their contact center agents. With 95% of all business attacks targeting your people as their way in, it is important for organizations to build a culture of security that can defend them just as well at the front line as they do in the server room.

We partner with clients to create and execute on that plan by evaluating their security awareness, delivering custom training and ensuring their people are an active part of the overall business health, security, and success.