contact MANAGEMENT

THE CUSTOMER EXPERIENCE MAGAZINE ISSUE 2

Oh Canada

Canada's place in the new era of Contact Centres

› Contact centres under attack

› Building people-focused contact centres

Under attack!

The contact centre's role in security management

Social engineering: Social engineering, in the context of information security, is understood to mean the art of manipulating people into performing actions or divulging confidential information. This is a type of confidence trick for the purpose of information gathering, fraud, or gaining computer system access. It differs from traditional cons in that often the attack is a mere step in a more complex fraud scheme ~ Wikipedia

By Katherine Thompson

We live in a world where information, communication and access is truly at our fingertips. Between the continued emergence of mobile applications and online resources, we are the generation of empowered consumers able to conduct our daily lives with more convenience and access than ever. But with that access comes inherent risks. The information we share, whether it's through the companies we do business with or through online social media sites, is quickly becoming a lucrative and sought after commodity. The experienced and professional hacker has many methods to access and extract this information. While online (cyber) and physical security tactics are most prevalent, the emerging strategy of social engineering is starting to capture the attention and concern of many in the business of protecting your information.

"How hackers hack—protecting yourself and your customers" was the topic of a recent Greater Toronto Contact Centre Association (GTACC) morning meeting hosted by the Peel Regional Police. The well-attended event attracted an interesting cross-section of industry and responsibilities, all sharing a mutual interest and concern in the growing demand for cybersecurity mechanisms. Derrick Webber, Penetration Testing and Forensics Team Lead at CGI presented a very entertaining and insightful look into the innovative and aggressive means professional hackers are using to gain access to your company's systems and data. Following the event, I had the opportunity to sit down with Derrick Webber to discuss the impact, responsibilities and opportunities the contact centre will play.

The emerging threat of social engineering

"There's a saying in our industry—amateurs attack systems and professionals attack people" says Webber. "We are seeing more attacks being carried out through human channels". Webber goes on to point out that one of the key areas being exploited is verification services. He references the recent hacking of the Associated Press Twitter account which falsely announced explosions at the White House that resulted in temporarily wiping out $136 billion in value from the Standard & Poor's 500 Index. While this exploit resulted in Twitter implementing upgraded online security, frontline verification methods still pose a significant threat to security.

The contact centre has a role to play in security management

While there are a growing number of acknowledged security breaches through social engineering, there are much more that go unreported. "Where we see an emerging role for the front line representative is being able to identify and track attempted breaches through channels like the phone and online means such as chat and social media sites" says Webber. "This would involve training representatives to be able to identify these attempts. By tracking and reporting this data companies will be better able to identify trends, adjust internal management protocols and protect important data." With the inevitable changes in global legislations surrounding breach management and reporting, Webber believes the investment in training your frontline staff will safeguard against legal action, severe penalties and loss of customer loyalty.

Communication is key but still lacking

Many companies have established protocols in place for the management of breach attempts, yet many overlook the role of the contact centre in managing the flow of communication both within an organization and to the customer. Legislative changes to PIPEDA open the door for the contact centre to play a much larger role in breach management, especially as it relates to time sensitive communication to those impacted by the breach. "From a compliance perspective, the need to communicate will be required. In terms of managing and monitoring social engineering attacks, the frontline representative can become your company's most important safeguard" says Webber.

Katherine Thompson *is a passionate and committed voice of the global BPO industry focusing on current and emerging trends that impact how customers engage, respond and commit to your company's brand.*

"The presentation for GTACC at Peel Regional Police Station was amazing. The focus of the session was on security and more importantly information security. I thought the speaker did an excellent job at showcasing the relevance of information security and made his examples applicable to all industries. The venue was excellent, audience participation was high, and the topic was extremely relevant for the current social/political climate. Kudos to a great job GTACC!"

~ Nygel Weishar, Sr. Manager - Scotiabank

"There was so much to learn from the Peel Police tour put on by the Greater Toronto Area Contact Centre Association. The lessons on cyber crimes and the criminals behind them were alarming and insightful. I have always ensured my client data is encrypted and secure and I walked away with a better understanding of how to continue to protect my own personal information (e.g. two factor authentication). In the "old" days we knew not to click on unknown attachments in emails, modern cyber-criminals have replaced the attachment attack with a seemingly harmless link from a friend or colleague who's computer has already been hacked. You click on the link from that friend or colleague and now cyber-criminals have full access to your computer (and all the databases and files connected to it). This, according to the experts in the demonstration, is the biggest risk to the security of business data. Cyber-criminals will use call centres as an avenue into customer accounts and agents are a first line of defence. Agents are often the first to receive a call from a customers when their account has been compromised. In both cases the call centre plays a very big role in defending the advances of cyber-criminals. The organizations that take this threat seriously and prepare front line agents for these situations will be in a better position to defend against these real threats to their customers and their data."

~Graham Kingma, President Imagen Business Solutions

Highlights from 2013 Internet Security Threat Report, Volume 18 Key Findings

- 42% increase in targeted attacks in 2012.
- 31% of all targeted attacks aimed at businesses with less than 250 employees.
- One waterhole attack infected 500 organizations in a single day.
- 14 zero-day vulnerabilities.
- 32% of all mobile threats steal information.
- A single threat infected 600,000 Macs in 2012.
- Spam volume continued to decrease, with 69% of all email being spam.
- The number of phishing sites spoofing social networking sites increased 125%.
- 5,291 new vulnerabilities discovered in 2012, 415 of them on mobile operating systems.

Source: Symantec Security Response