CONTACT CENTER PIPELINE
MAY 2018

A 360-DEGREE APPROACH TO CONTACT CENTER SECURITY

"It's crucial that employees are empowered to play an active part in maintaining contact center security. After all, they witness more of what takes place on the call center floor than supervisors."

Contact Center Pipeline

A 360-DEGREE APPROACH TO CONTACT CENTER SECURITY

Scrutinize your center from the inside out to safeguard security.

BY Brian Burke, GCG

A group of employees heads out for dinner after work. Over drinks, they discuss a banking case they are working on, not paying attention to their volume or the people at surrounding tables. Someone overhears their conversation and identifies their company from their name badges.

A new employee sneaks his cell phone onto the contact center floor. After checking his text messages, he places the phone back in his pocket, inadvertently pressing a button that dials an acquaintance. The phone records his next conversation with a caller where personally identifiable information is discussed.

A contact center relocates to the first floor of a new business park. In an effort to maximize space, some work stations are positioned so that the computer screens face the exterior walls. After hours, the light coming from inside the center makes the content on the computer screens visible.

These are just a few of examples that illustrate how easily contact center security can be compromised. With contact centers supporting nearly every industry, from retail and banking to law and healthcare, they often serve as a central hub for privileged and sensitive information. Much of the data that filters through them on a daily basis is regulated, making its protection and security of utmost concern for operations leaders.

Research suggests that insider threats, whether malicious or unintentional, are among the most common causes of security and data breach. As a result, responsibility falls squarely on contact center managers to ensure that internal threats stemming from people, infrastructure and operations are minimized at every turn.

People

Employees are a contact center's biggest security threat. According to the 2017 Insider Threat Intelligence Report, insider threats fall into three categories—malicious users, negligent users and infiltrators—with negligence accounting for nearly 70% of insider incidents. Regardless of whether employee mistakes are deliberate or careless, they can cost a contact center millions of dollars in remediation and cause irreparable damage to its reputation.

While employees are a contact center's biggest security threat, they are also its biggest asset. Customer service representatives (CSRs) are a manager's eyes and ears on the floor and a company's first line of defense against data breaches, making it crucial that they understand security expectations, remain engaged throughout their tenure with the company, and are empowered to make security a personal objective.

Building a culture of security begins during onboarding, when CSRs first learn how their role factors into the greater risk management function of the company. Oftentimes, new team members' responsibilities are too narrowly defined during training, limited to log-in procedures and call scripts, and they fail to exit training with a comprehensive understanding of the bigger picture. This creates a breeding ground for negligent behavior.

Training represents a prime opportunity to show new team members what is at risk and how they can help create and maintain a secure contact center. All contact center training sessions, whether conducted over several hours or several weeks, should incorporate a broad discussion of the company, including what it does, whom it serves, where new team members fit into the puzzle, and why maintaining secure operations is critical to its success. From there, CSRs can make a more meaningful connection between their day-to-day job function and the security protocols they've been exposed to during training.

Onboarding, however, is only one part of the equation. Unless the concepts covered in training are reinforced every day, they become little more than boxes to be checked. Supervisors should set aside time each day to coach employees on risky behaviors and to remind them how their tasks influence larger security efforts. Managers can help eliminate the potential for agent complacency by staying abreast of the latest security threats and breach tactics, and discussing those with their team members in real time. Perhaps most important, they should look for and reward employees who model desired behavior and make security a priority.

Finally, it's crucial to empower CSRs to play an active part in maintaining contact center security. After all, they witness more of what takes place on the call center floor than supervisors. Empowered and engaged CSRs can serve as an extension of the management team, monitoring their surroundings and reporting concerns to contact center leadership. In addition to reporting, all team members should be authorized to question and address any behaviors or attitudes that do not align with or promote the company's security efforts, such as stopping people they do not recognize within the four walls of the center. That level of participation is a key component to creating and sustaining a culture of security.

Infrastructure

A contact center's infrastructure is foundational to promoting a strong culture; in fact, a strong culture cannot emerge unless employees are working within an infrastructure that

supports and echoes their commitment to security. However, in the design and implementation of contact center infrastructure, a company's effort to maximize space and efficiency can unknowingly cause security considerations to take a back seat.

Beginning from the outside, consider not only how secure the contact center is during the day, but also how secure it feels at night. Are parking lots well lit, and are mechanisms in place to promote the safety of employees, such as security cameras and policies requiring employees to leave in groups after hours? Are contracts with landscaping and snow removal companies kept up to date, and does window tinting account for changes in lighting that occur naturally throughout the day, prohibiting viewing inside the contact center at night?

Inside the contact center, are work spaces arranged such that computer screens are not facing exterior windows, and are work stations disconnected and disarmed when not in use? Does the physical space and floor plan minimize the chances an employee will wander into locations where sensitive programs are underway? Break areas, rest rooms and employee lockers, for example, should be located in common spaces to control employee traffic patterns, and work areas should be compartmentalized in a manner that requires key card entry valid only for agents approved to work on a specific project. Further, work areas, when not in use and under routine surveillance, should be locked down and accessible only by managers.

Security infrastructure should extend beyond the physical space to include digital considerations such as web access, downloading and printing. Those facilities that authorize agents to access printers should ensure their equipment is outfitted with a monitoring system that requires multiple levels of verification and records activity, up to and including the attempted use of USB or other external hard drives. Both internal and external communications should be encrypted in case of interception, and outside media should be filtered through the IT department to determine authenticity before it can be uploaded to contact center networks. Finally, all computers should be routinely checked to ensure that internet access is disabled and networks are secured.

A scrutinous approach to the security infrastructure within the contact center is not a one-time event. In fact, in an increasingly digitized landscape, managers must remain keenly aware of developments and advancements in breach strategies and committed to making real-time adjustments and investments to maintain an environment that puts security first.

Operations + Procedures

Good contact center managers assume their employees are motivated and committed, but great contact center managers know that all variables in the security equation must be accounted for. This starts with comprehensive operational policies and procedures that encourage positive behavior and enable agents to become champions for security.

Policies introduced during training and reinforced throughout employment should include objective guidelines that expressly prohibit cellular devices on the contact center floor. A tangible threat to privacy and security, the use of mobile phones—smart or otherwise—should be grounds for immediate dismissal, no questions asked. Whenever possible, the use of pens and pencils at workstations should be discouraged, as they may promote mindless scribbling that could unwittingly expose sensitive caller information. Employees should agree to limit their discussion of all programs and projects to supervisors and managers, especially in casual settings, including the break room. Further, company badges should be removed immediately upon exit to prevent loss or theft, which, in combination with small details about a project, could enable an impersonator to portray an authorized agent and gain entry to the building.

Social media policies that outline appropriate online behavior should also be enforced, as agents, whether they realize it or not, are online representatives of the contact center. Social media content that identifies, even loosely, clients, companies, programs, or fellow employees should be banned. Additionally, in coaching sessions, managers should remind employees of the lesser known dangers inherent to social media. For example, popular social media surveys that circulate on Facebook may encourage agents to publicly share personal information, which is often used in the design of company passwords.

Password protection remains a chief operational concern for contact center managers as a large portion of security hacks happen when passwords are issued and changed. Initial employee logins and passwords should be distributed in person during training to avoid interception in external communications and, once agents are in place, they should be required to change passwords at regular intervals. As an added level of security, password updates for various access points, such as company computers and software programs, should be done on an alternating cycle to discourage the use of a singular password across several platforms.

Unfortunately, security policies and procedures alone cannot guarantee compliance. For that reason, it is advisable for contact center leadership to maintain formal channels for employees to report security concerns. In addition to managers being available and committed to open-door policies, a company email address, monitored suggestion box, or anonymous hotline will go a long way toward reinforcing the security culture, and may promote agents, especially those new to the company, to be forthcoming with concerns.

In this day and age, accounting for all the security challenges and threats can be overwhelming for contact center leadership. Contact center managers should make it a daily practice to explore their operations from the inside out, intentionally scrutinizing their infrastructure, their people and their policies and procedures to ensure they promote and safeguard security. And when they fall short, they should react quickly, prioritizing those shortcomings above all other matters. After all, without secure operations, there are no other matters.

Brian Burke is Senior Vice President of Operations for GCG, a leading global provider of legal administration and business solutions. Burke oversees GCG's 60,000-square-foot Mail, Call and Processing Center in Dublin, Ohio, which supports the hundreds of active class action settlement administrations, restructuring and bankruptcy administrations, and mass tort settlement programs GCG has in progress at any given time. (www.choosegcg.com)

FOLLOW ME:
@GCGNews

CONNECT WITH PIPELINE

 @SusanHash • @CCPipeline

 youtube.com/ccPipeline

 linkd.in/17M5rKM

About Contact Center Pipeline

Contact Center Pipeline is a monthly instructional journal focused on driving business success through effective contact center direction and decisions. Each issue contains informative articles, case studies, best practices, research and coverage of trends that impact the customer experience. Our writers and contributors are well-known industry experts with a unique understanding of how to optimize resources and maximize the value the organization provides to its customers.

To learn more, visit: www.contactcenterpipeline.com

 Download complete issues, articles, white papers, and more at http://bit.ly/14bq01k

PIPELINE PUBLISHING GROUP, INC. PO Box 3467, Annapolis, MD 21403 • (443) 909-6951 • info@contactcenterpipeline.com