Contact Center Security

Understanding and Managing Risk

Introduction

As a contact center manager, you're no stranger to risk. Every day, you face the risk of a compliance violation, the risk of financial fraud, the risk of data breach and the risk of identity theft, just to name a few. But even as you face these modern security realities, you must also provide the contact center with advanced technologies that enable agents to deliver unparalleled personalized service. How do you reconcile ensuring that the agent "knows" the customer to create a personal experience with the need to secure private information? In this white paper, we explore the various ways to address risk as well as identify the types of risk that come with customer engagement platforms.

Understanding Risk

Negative risk is a normal part of doing business, and it's present everywhere: from the corporate board room to the reception area – and everywhere in between. The issue lies not in risk's existence but in your response to it. Many times, the very action that presents a risk also presents a business opportunity. The key is to respond to risks in a way that improves opportunities while reducing threats.

There are four ways you can respond to risk:

- **Acceptance –** Accept the risk as-is.
- **Avoidance –** Avoid the risk by either eliminating the threat or choosing to not take the action associated with the risk.
- **Transference –** Transfer the risk to a third party, such as an insurance company or a third-party outsourcer.
- **Mitigation –** Take action to reduce the probability or impact of a threat.

It's important to note that only through avoidance do you steer clear of risk entirely. Risk is still present with acceptance, transference and mitigation. It's just a matter of how much risk you're exposed to and in what manner.

Contact centers face a number of risks due to the sensitive nature of the data they receive, work with, store and process. Let's start with financial transactions. Organizations are required to comply with the Payment Card Industry Data Security Standard (PCI-DSS), a set of standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment.

Of course, where's there's financial data there's also risk of financial fraud, and the contact center is no different. Fraudsters have been known to use social engineering in an attempt to get account information, which they then use to complete fraudulent activity via another channel. This isn't too difficult if the contact center authenticates callers using basic information (like the account holder's phone number, first school, address or date of birth) that can be obtained from an unrelated data breach.

Financial fraud isn't limited to people posing as your customers. Agents themselves pose a risk to your organization if they are taking and processing credit cards. While organizations want to trust their number one asset – their people – the fact of the matter is your agents are human and thus largely unpredictable. There will always be some level of risk of internal financial fraud as long as humans are involved and the opportunity is present.

A data breach is another issue altogether. Contact centers take and store an increasing amount of personally identifiable information (PII). It used to be that basic information found in the phone book wasn't considered sensitive. However, now that data is considered valuable because it can be correlated with other data and used to commit financial fraud and/or tarnish an individual's reputation.

Large-scale data breaches are a real threat to organizations, and many companies aren't aware that they are being attacked. Cyber attackers use sophisticated threats that quietly bypass traditional security controls and exfiltrate data from corporate systems. It can takes weeks or months for victim companies to detect an attack and often after the damage has been done. The data from these attacks is typically sold to other criminals who use it to commit financial fraud or identity theft.

Full PCI compliance doesn't render your organization immune to financial fraud or a data breach. In fact, your organization can be 100% PCI-compliant and validated, and still suffer a cardholder data breach. What's more, you can be subject to fines and be prohibited from accepting credit cards by a merchant's card provider. In all of these scenarios, the company suffers from a damaged reputation, loss of revenue, loss of customer and shareholder trust, reduced share value and increased costs.

Risk Meets Customer Service

By themselves, these risks seem fairly simple to address. Your organization can avoid PCI risks by prohibiting financial transactions. Or maybe you severely limit the type and amount of customer data you collect. The problem is that contact center managers must contend with a number of trends in the customer service industry that eliminate these options and complicate risk management.

We know the telephone is no longer the only means of communicating with your company. In addition to speaking directly to an agent, customers can communicate via social media, email, web chat, web forms, online surveys and more. Aditionally, customers expect consistent and proactive service across all of these channels (and more, as they become available) in what is known as omni- channel customer engagement.

Omnichannel customer engagement implies that each communication channel is aware of the others and the activity at any given one is informed by the customer's past activity. So, for example, if a customer returns the same style t-shirt twice, in two different sizes, the system knows to recommend a t-shirt in a different cut – or maybe make a different suggestion altogether. Although omnichannel customer engagement technology has reached a level of maturity, the ability to deliver this type of proactive service remains a competitive differentiator in many industries.

Personalization goes hand-in-hand with omnichannel customer engagement. Every touch point needs to know who the customer is, their history and preferences. You need to be certain that you authenticate the customer before you deliver any sensitive data via a given channel. Any data sent to and from the customer must be protected. And security policies must be consistently applied throughout your customer engagement platform to ensure that no single channel becomes an attack vector.

Even as customers want personalized service across multiple communication channels, they're also increasingly aware of privacy issues. You must be sensitive about the use of their data. There's a fine line between making an intelligent guess as to your customer's needs and making a creepy "big brother" move that drives customers away. In addition, you must reassure customers that you're taking the appropriate steps to protect the data they entrust to you. Frequent news headlines of data breaches keep the threats of financial fraud and identity theft front-and-center in customers' minds.

Meanwhile, as systems of engagement move to the cloud, the technology to enable omnichannel customer engagement has become cloud-based, too. If organizations want to benefit from cutting edge capabilities – like integration with heterogeneous legacy systems, unification of distributed customer service teams, reliability and scalability – then they

must host their platform in the cloud. However, that could mean giving up some visibility into system controls, security and regulatory compliance efforts.

Today's contact center manager faces a variety of conflicting mandates with no clear direction on how to appropriately manage risk.

A Customer Engagement Platform for the Modern Contact Center

There is lot of noise in the crowded customer engagement platform marketplace around the concept of omnichannel. However, as previously stated, the technology is not new. Mature providers that have offered omnichannel capabilities for more than a decade have built risk-averse platforms. It's vital that organizations look for such a provider because, as the focal point of your omnichannel efforts, the customer engagement platform must play an active role in helping the contact center manage risk. If it's not actively managing risk, then it's increasing your risk.

Here are two specific ways in which an omnichannel customer engagement platform can reduce your risk:

MOVE FINANCIAL TRANSACTIONS OUTSIDE OF THE CONTACT CENTER

Managing financial transactions is unavoidable. You have little choice but to accept credit card payments and must therefore (1) comply with PCI standards and (2) protect cardholder data against security and privacy breaches. A mature platform provider can address these requirements by providing a safe payment transaction platform outside of the contact center environment. These solutions combine the following elements:

- A multi-modal connection that allows the contact center agent to service the customer on the phone, while simultaneously sending a link via text message or email to a microsite that manages the transfer of funds outside of the contact center
- A connection to a secure, external Interactive Voice Response System for customers who wish to conduct their transaction in a voice-enabled environment
- Routing logic to a payment gateway that transmits data directly and securely between the customer's account, bank account and card providers.

Removing the payment process from the contact center enables organizations to significantly reduce PCI scope and audit requirements. This not only saves time and cost, it also reduces the risk of a compliance violation, as well as financial fraud, identity theft and data breach because agents can't access the data and the data isn't stored on your premises. This same functionality can also be used for other sensitive transactions that must be available to customers via the contact center.

PARTNER WITH A SECURE CLOUD PROVIDER

In addition to being an expert in PCI compliance, your platform provider should be an expert in securing the infrastructure on which the platform runs. A mature provider has years of experience securing hosted environments for a variety of companies in a variety of industries. Because one-size-cloud does not fit all, the provider should offer several choices of platform configuration based on your business requirements and risk tolerance.

If scale, reliability and flexibility are your primary concerns, the provider should implement mitigation controls to enable you to take advantage of the public cloud while reducing risk. Alternately, providers can also set up a virtual private cloud that enables you to leverage the public cloud but with dedicated instances. Finally, you can take a hybrid approach in which some of your infrastructure runs on premises to enable IT to maintain control of critical data assets, then bridge into a virtual private cloud for processing power.

USAN's Omnichannel History

Today, USAN delivers secure, omnichannel solutions for large enterprises in a number of industries. It started in 2001 when we built a flexible, fault-tolerant platform to combine BPM, CRM, business intelligence, content management, analytics and unique multichannel delivery into a fully unified customer engagement solution for a major satellite provider as well as several financial services payment processors. That platform became what is known today as USAN Metaphor Engage, which powers USAN's Metaphor Secure Contact Center family of products.

We believe that delivering a superior omnichannel customer experience is only worthwhile if data is protected and contact center risks are sufficiently managed. Security is intelligently designed into the Metaphor product suite to enable agents to deliver a seamless customer experience as efficiently as possible while protecting your customer's data. USAN has over 20 years of experience in protecting PCI, PII and healthcare data. We embrace the concept of managed risk and work with our clients to create a measureable and maintainable approach to risk mitigation and avoidance to ensure your customer's data is protected.

Metaphor Engage integrates various channels (web, SMS, social and phone) with your backend systems to offer customers a seamless experience. It unifies and protects data across all channels to consistently deliver personal and relevant customer interactions while improving service and satisfaction levels. Its unique capabilities let you implement a solid and scalable infrastructure faster and with less risk.

About USAN

USAN helps companies profitably engage customers and deliver amazing omnichannel experiences with the industry's best cloud and hybrid customer engagement solution. From traditional telephone interactions to web-based communications including chat, email and social, USAN's portfolio of contact center applications gives businesses infinite flexibility in the way they engage customers across channels.

In addition to hosted ACD, IVR, WFM, Quality Management and Agent Desktop, USAN offers back-office integration and business process automation powered by a sophisticated omnichannel rules and workflow engine. All built upon a fifth-generation, carrier-grade infrastructure that delivers the highest availability in the industry, with proven scalability to support the largest enterprises.

3080 Northwoods Circle
Norcross, GA 30071

www.usan.com

office 770.729.1449
fax 770.729.8589