ConvergeOne | AVAYA

A CISO'S SIX STEPS TO SECURING AN EXCELLENT CUSTOMER EXPERIENCE

2020

In today's world, sharing sensitive data over the internet is an expected everyday occurrence. Sure, you hear about the large-scale data security breaches that affect countless enterprises, but you just hope it won't happen to you. The problem is that customers expect their data to remain secure. A breach could significantly impact their privacy, not to mention their trust in your organization. It's important that you pause and ask yourself these questions: What are our most valuable and sensitive digital assets, and how well are we truly protected against attack?

The best place to start in providing a more secure customer experience is the office of the Chief Information Security Officer (CISO). In this white paper, we interviewed ConvergeOne's Chief Information Security Officer, Collin Buechler, and Senior Director, Customer Experience Strategy, Kathy Sobus to determine the steps to ensuring a secure customer experience.

Overview

Raise your hand if you're guilty of sending secure information using your cellular device. Don't worry—we all do it, despite the inherent risk involved in transmitting sensitive information across cellular and data-driven networks. However, this could leave not only your organization, but also your customers' personal information, at risk. Customers want to feel safe interacting with your business. A critical component of an excellent customer experience involves ensuring the safety of your customers' data.

Let's take a step back and first discuss the importance of a strong cybersecurity program. In its latest Global Risks Report, the World Economic Forum rated a large-scale cybersecurity breach as one of the five most serious risks facing the world today – and the scale of the threat is expanding rapidly. In 2018, the US Intelligence Community Worldwide Threat Assessment identified cybersecurity as the #1 threat for the 3rd year in a row. Cybersecurity Ventures estimates that by 2021, the financial impact of cybersecurity breaches globally will reach $6 trillion, double the 2015 total.

Coping with digital challenges and mitigating these risks is an increasingly urgent focus of organizations around the world. To gain cyber resilience and fight cybercrime, companies are boosting their investment in cybersecurity. Of the 1,200 C-suite leaders polled by EY for its 2018 Global Information Security Survey, 70% responded that they expect to increase their corporate security funding by 25% or more in the coming years.

Today, regulators, lawmakers and customers alike demand that companies take steps to improve their defenses. As a result, organizations are devoting more and more time to developing crisis response plans for potential attacks. Two years ago, IBM opened one of the country's first cybersecurity sites in Cambridge, Massachusetts, to help companies learn how to respond to simulated cyber-attacks. The company describes the experience as "a game of Clue mixed with a Disney roller-coaster ride."

A Secure Customer Experience

The best place to start in providing a more secure customer experience is the office of the Chief Information Security Officer (CISO). The CISO is a Cybersecurity expert assisting organizations to successfully implement their security and privacy strategies. Their focus is on business imperatives, protecting IP and the brand, achieving or maintaining regulatory compliance, establishing a culture of security and ensuring that a resilient, adaptive security strategy exists.

That's why we interviewed ConvergeOne's Chief Information Security Officer, Collin Buechler, to determine the steps to ensuring a secure customer experience.

According to Buechler, "every day is a new threat landscape." New and emerging challenges – including risks generated by the use of mobile devices, the vast volume of evolving threats and vulnerabilities, and the difficulty of complying with the expanding regulatory climate – have added to the complexity of fending off cyber-attacks that affect sensitive customer information.

Though consumers are typically aware of the risks, they believe that digital channels are mostly secure. In reality, hackers are everywhere, and the majority of breaches are caused by an attack on the company's people rather than its technology. An entire ecosystem exists on the black market to develop and sell viruses, which are implanted via malicious emails, phishing, and other social engineering methods.

For example, a large U.S. based financial services firm suffered a security breach in 2018 that exposed the personal information of thousands of its customers. The hackers were able to gain access to the data by impersonating financial representatives and tricking the firm's information technology help desk into resetting passwords. This is an example of "vishing" (a portmanteau of "voice" and "phishing") – whereby a malicious actor impersonates someone over the phone to trick others into providing customer or personal information – and it's becoming all too common. In fact, 60% of account takeover incidents involve the contact center, and the impact of these attacks is tremendous: Identity fraudsters stole $16 billion from 15.4 million victims in the U.S. last year alone.

The attack on this financial services firm illustrates an important shift in how companies need to approach cybersecurity. We call this shift "posture over product." What this means is that cybersecurity needs to be a balance of people, process and technology. Good security is not found in a "box" or any single product on the market. Good security is about having a negotiable feel for people and how they learn best, processes and policies that are fully understood, adopted and yield consistent results, and technology that is field validated, not just innovative or unique. Lastly, cybersecurity should be right there with concepts like corporate governance and safety, fully ingrained in the culture of the organization, and with a strong setting of "tone at the top."

How can you effectively safeguard the information your customers entrust in your company, as well as protect proprietary material and data? Begin your journey to a more secure customer experience by following these six steps.

STEP 1: START WITH A CISO

In 1994, following a series of dramatic cyber-attacks from infamous Russian hacker Vladimir Levin, Citigroup created the world's first formal cybersecurity executive office position by naming Steve Katz its CISO. Katz had organized and managed the information security program at JP Morgan and was well known in the industry as a pioneer in the cybersecurity field.

In the ensuing twenty-five years, the role of CISO has evolved significantly. They should be and often are executives who translate technical terms to business terms and vice-versa. They understand business, security and privacy equally well, thinking in terms of risk and monetary impact (value at risk and cost of control). They are extremely well-versed in corporate and technology strategy, and they believe in clear metrics and set priorities based upon them.

At larger companies, CISOs typically oversee a team of security professionals that work for the company. Smaller firms more often outsource security oversight by hiring a virtual or fractional Chief Information Security officer, getting the same capabilities as a full-time experienced. CISO but for substantially less cost.

Top CISO's bring or develop a model for risk and an applied formula that answers the questions of, "Are we doing the right things, enough of the right things and in the right prioritization order?"

If you want to get serious about cybersecurity, it's time to include the CISO as a trusted member of your executive leadership team.

STEP 2: INVOLVE SENIOR LEADERSHIP

Between the SEC's requirement that publicly traded companies disclose material information about security events, and the increasingly frequent news headlines about data breaches, senior executives and corporate boards are more involved than ever in how organizations manage and implement their security programs. After all, just one serious cybersecurity incident could derail the growth and profitability of an entire company—and potentially cost them their jobs. "My leadership team is completely behind me," said Buechler. "They take security seriously and that is the single most important thing."

If your senior leaders aren't engaged, it's time to bring them into the fold. Buechler suggested avoiding scare tactics: "Discussing corporate security can cause alarm because many believe the best way to sell it is to create fear and uncertainty. I don't like that approach. What we should be doing is providing our executives with information clearly and calmly so that they understand what is being done and why it is important, but not in scary terms."

STEP 3: ADOPT A RISK-BASED APPROACH

Over the last two decades, CISOs have shifted their focus from the implementation and management of cybersecurity control technology to a consultative, business-process-aware risk management approach. CISOs and the organizations they support must borrow from their brethren in auditing roles, in that information must be translated and executed via a program that manages risk at the digital asset level, but focused on cyber-resiliency and how to increase it. The majority of what comprises good security posture is foundational in nature, but like the Pareto Principle, the 20% that is differentiated between you and your competitors often makes the difference between being victimized and being able to detect, then ward off attacks.

STEP 4: PARTNER WITH CUSTOMERS

“ConvergeOne is not a target because we are ConvergeOne,” said Buechler. “We are a target because of the customers we serve.”

Where traditionally CISOs were expected to possess keen technical knowledge, today they must also have strong consensus-building, influencing, and communication skills both inside and external to the organization.

Strong relationships within an organization are critical to implementing a successful risk-based approach. “I consider myself a consultant and a partner, offering our businesses and customers assistance and guidance,” said Buechler. He and his team work closely with ConvergeOne’s Customer Success Center (CSC) – a customer-facing contact center team – to address customer needs and concerns. “We are often the first to discover a problem on a customer’s network because we can track vulnerabilities on phone systems, working hand-in-hand with the CSC,” said Buechler.

While ConvergeOne is a large company, it has acquired several smaller companies over the years. Buechler noted that working with smaller companies brings its own challenges: “Smaller companies do not have the same emphasis on cybersecurity, though ironically it is actually easier for hackers to get in through the smaller door.” Buechler explained that establishing policies and frameworks for industry best practices—as well as a blueprint for how to interact with customers and their data—help to decrease the risk of being blindsided by serious security issues. “We have over 14,000 customers, so we partner with them to make sure we are meeting their security needs, constantly monitoring practices and controls, and listening to their questions and concerns,” Buechler added.

STEP 5: STAY ON TOP OF REGULATIONS AND LEGISLATION

One of the most challenging aspects of information security management today is the shifting regulatory landscape. It is increasingly difficult for companies to stay ahead of how emerging state privacy legislation impacts not only their own systems, but also those of their customers and partners. To further complicate matters, each state has its own regulations that sometimes conflict with regulations in other states. Currently, over 100 different proposals regarding cybersecurity are being considered in statehouses across the country, and 15 states have passed data privacy laws.

Moreover, the EU’s General Data Protection Regulation now brings forth the notion of privacy by design and potentially the need to also have a Data Protection Officer (DPO) in addition to your CISO has caught many organizations by surprise.

“There are 78 different regulations to consider, just for ConvergeOne, before we even connect with a customer who has its own unique regulatory suite to manage,” Buechler explained. A close partnership with legal and compliance teams – both internally and with customers – is essential to managing all touchpoints, assessing compliance, and understanding your liability as a company and with customers in the event of security issues.

STEP 6: TAKE ADVANTAGE OF EMERGING TECHNOLOGIES

Biometric authentication – including facial, thumbprint, or voice biometrics – has recently been gaining popularity. Just a few short years ago, the accuracy rate for voice authentication was 86-90%. Now, it is anywhere from 93-97% accurate, depending on the audio length and if the recording is in mono or stereo.

With voice biometrics, authentication takes place in the first few seconds of the call. Both enrollment and authentication can be passive and happen in the background, without disrupting the flow of the call. Most, if not all, of the authentication process is therefore eliminated, saving an average of 40 seconds per call. Not only are you providing a more effortless and efficient customer experience, but you've also got a built in return on investment.

Use of AI – whether augmented or artificial intelligence – also bolsters the security of your contact center. As we shared earlier, most cyber-attacks are targeting human error, so if there is little to no human intervention, there is less opportunity for fraud to occur in your contact center.

Take Action. ConvergeOne Can Help.

Making the shift toward a more cyber-aware and secure culture can be a very onerous task for your company to take on. The same is true for determining the right technology to support a secure customer experience. That's why you should work with a proven integrator like ConvergeOne to ensure you have the right mix of customer experience and cybersecurity solutions – ones that positively impact your security posture, are 100% compliant, use the latest field validated technologies, and reduce human error and breaches.

Get Started Today.

Take the first step by registering for a demo, assessment, workshop, or proof of concept with ConvergeOne: convergeone.com/letstalk

About ConvergeOne

ConvergeOne is a leading IT services provider of collaboration and technology solutions for large and medium enterprises.

About Avaya

Avaya elevates communications to the next generation of engagement, connecting organizations to their customers, workforce, and communities with secure, intelligent experiences that matter.

ConvergeOne | AVAYA