CISO COUNCIL SERIES: SECURING CUSTOMER IDENTITY DATA

A special publication from Ping Identity's CISO Advisory Council

WHITE PAPER

TABLE OF CONTENTS

INTRODUCTION

Ping Identity's CISO Advisory Council is comprised of CISOs and security leaders from enterprise organizations, including: Chris Gullett, VP of Information Security for Allegiant Air; Krizi Trivisani, CISO for American Red Cross; Diane Ball, CISO for BCBS Tennessee; Harshal Mehta, CISO for Carlson Wagonlit; Karl Mattson, CISO for City National Bank; Sam Masiello, CISO for Gates Corporation; Michael Strong, CISO for GCI; Rich Gay, CISO for PowerSchool Group LLC; Mark Freed, CISO for TechnipFMC; Adrian Mayers, CISO for Vertafore; and Grieg Arnold, CISO for Vista Equity Partners.

73%

of consumers say a good experience is key to their brand loyalty.[1]

32%

of consumers will leave a brand they love after just one bad experience.[2]

Customer identity data can be invaluable to your ongoing business success as you navigate digital transformation and modernization initiatives. You can use this data to gain critical insights into trends and shifts in the market, providing the information you need to bring the right products and services to market.

Customer identity data can also be leveraged to deliver the type of experiences your customers want and need. For example, you can use it to increase personalization by delivering the right offer to the right customer at the right time.

But in an age of increasing regulations around privacy and consent, you must be careful that you don't prioritize improvements in your customers' experience over judicious management and use of their personal information. Regulations like GDPR and others impose steep fines for non-compliance. In early 2019, Google was fined $57M for failing to comply with GDPR—a penalty 3X higher than any HIPAA penalty issued over the last eight years. While Google is disputing the infraction, their case underscores the reality that today's organizations must walk a fine line when it comes to managing and securing customer data.

The risk of being fined for non-compliance is just the tip of the iceberg. The loss of customers and revenue, as well as the reputational damage that results from a data or privacy breach often have a bigger and more sustained impact.

While digital transformation initiatives offer immense potential for growth, they also present challenges and risks, the scope and scale of which are worthy of increased attention from the C-suite and additional investment in data protection. This paper provides guidance in navigating these risks and challenges, specifically with regard to securing customer identity data.

TAKING OWNERSHIP OF CUSTOMER IDENTITY DATA

The responsibility for balancing workforce security and user experience has long been the domain of corporate security and identity personnel. When it comes to your customers, however, the matter of ownership is more complex. Because of the revenue implications, your organization's relationship with customers is often viewed as a cross-functional responsibility. Often, marketing functions ultimately own the responsibility for customer identity data and are focused on delivering a strong and consistent brand experience.

But the management of customer identity data can't be overlooked or treated as an afterthought. Doing so can result in security and privacy deficits that put customer data—and your organization's future—at risk. Instead, security leaders must take a proactive role in ensuring the security of customer data and educating marketing stakeholders about both the risks and advantages of customer identity solutions.

While enforcing strong security was previously at odds with delivering seamless experiences, modern identity solutions allow you to strike the perfect balance. You're able to take the lead by not only educating marketing and other stakeholders about the importance of securing customer identities, but also by demonstrating how customer identity and access management (IAM) tools can actually enhance the customer experience.

At the least, these solutions should help you ensure your users are secure while removing unnecessary security friction. But the more compelling arguments often center on solving complex business problems with solutions rooted in security. For example, some organizations, like those that follow, must manage complex identity challenges, including managing access for users that are both customers and employees or business partners, as well as managing identities for minors and their guardians.

BlueCross BlueShield of Tennessee's (BCBST) employees are often health plan members (effectively customers) as well. BCBST's health plan brokers and healthcare providers might also be plan members. To deliver a frictionless experience, BCBST needs the ability to provide each user with a single identity. But to ensure data security and compliance, they also need to enforce different access policies for that single identity, depending upon how the user is using their system. Read the case study.

Similarly, a single person involved in the American Red Cross may be a donor, employee and/or a volunteer. Depending on the role they're in at the time, their access rights must be different.

Allegiant Air's employees are often contractors and may be working on multiple contracts with different contracting firms at the same time. These employees need to be provided different levels of access depending on the contract and contracting firm. Read the case study.

PowerSchool, a leading provider of K-12 education application technology supporting more than 45 million students in 70+ countries, must manage student identities. Managing child identities and their associated credentials—not to mention managing access permissions which can be impacted by marriage, divorce and other guardianship changes—presents a complex identity challenge.

LOOKING BEYOND COMPLIANCE TO COMPETITIVE ADVANTAGE

Little more than a decade ago, the prospect of a new wave of consumers who would shop almost exclusively online was unthinkable. Is it that hard then to imagine a world where those same consumers only interact online in places they feel secure and with companies they trust? Collectively, we believe that companies who prove their worth by ensuring that customer data remains secure and private over the long term will possess a key differentiator in the digital economy. And many industry experts and analysts agree.

But with new data privacy regulations emerging in the U.S. and beyond, including state and industry-specific ones (e.g., the NYDFS Cybersecurity Regulation), staying ahead of the wave can be a challenging task. We believe that at some point U.S. data privacy regulations will converge to exist at the federal level. But until that happens, organizations with flexible solutions to solve for data privacy concerns—not those custom built to comply with individual regulations—will gain a competitive advantage.

70%

of consumers would buy more online if retailers assured them their financial and personal data will be safe.[2]

Regardless of what happens in the future, there are many commonalities among privacy statutes today, even those developed on separate continents, that make compliance more universal and attainable than may meet the eye.

These commonalities combined with the opportunity to be more competitive—and of course avoid penalties for non-compliance—provide more than enough reasons for security and identity teams to step up and assume ownership of customer identity data, wherever it may reside.

SOLIDIFYING YOUR FUTURE WITH SECURITY AND PRIVACY BY DESIGN

Truly owning customer identity data requires more than just assuming control of its use and management. You must design security and privacy into customer experiences from the beginning. Doing so will enable you to take on any initiative—currently planned or as yet unknown—with greater speed and confidence.

When you have core security and privacy controls in place, you can be free from worries about which collected customer attributes need to be anonymized or obfuscated as these decisions will already be made with controls in place to enforce them. You can provide customers with detailed consent policies about the use and sharing of their data, as well as the ability to track and view details surrounding their opt-ins and opt-outs of data collection and sharing agreements.

While expectations around secure access, data privacy and consent are still taking hold in the broader market, the future state demands are already pressing organizations to consider how these functions will be managed. The traditional approach of rules and policy-based engines can't scale to address the diversity of use cases and the sheer volume of customer identities that companies will be managing.

The business case for truly secure and private customer identity data grows stronger each day. To address these new requirements, we anticipate a significant increase in both the development and utilization of advanced analytics like artificial intelligence (AI) and machine learning.

By allowing the application of entitlements and accesses to be automated, AI has the potential to further strengthen security while streamlining the user experience. In the meantime, though, there are steps you can take right now to secure your customer identity data.

FIVE STEPS TO SECURE CUSTOMER IDENTITIES

1. Know Your Current State

Map all the places where your customer identities live today. Then evaluate whether the controls in place are adequate to ensure access is secure in all scenarios where this data is accessed now and in the future. Many organizations find that customer identity data is accessible under circumstances and through channels of which they weren't previously aware. Some of these include access through legitimate channels, but on unmanaged devices. Others include access directly from API interfaces, previously believed to be secured by obfuscating API access within the UI of a web application.

2. Take Ownership

Assign ownership of the function of securing customer identity data to the team that has the best capabilities to safeguard and protect both that data and your customers. It does not matter so much which team this is, (security, a central identity function, IT or another team), as long as there is consensus on who will own it, and support from all key stakeholders. This team must be involved in decisions surrounding who gets access and by what means. This includes a review during the onboarding of new technologies (e.g. SaaS apps, APIs) and partnerships (e.g. research, supply chain) which ultimately require the exposure of customer data.

3. Build Your Strategy

Develop a strategy to unify your customer data into a single source, or federate your customer identity data from multiple sources. This will yield increased security value by shrinking your attack surface, improve the customer experience with a single login to all of your digital properties, simplify and reduce the administrative burden, and will allow you to move with greater speed and agility to meet your customer's trust-based demands.

4. Define Your Process

Clarify how you'll operate moving forward. Governance is critical to maintaining and continually improving all the work that you've done in discovery, assigning ownership and building a strategy. Outline common ways new paths to customer data are created so steward in any department know when to involve the security team. Train and communicate to the various stakeholders on this governance process, and get their buy-in to avoid painful projects down the road.

5. Authenticate, Authenticate, Authenticate

Providing customers with access to their data with the highest confidence, but lowest friction is the goal. Implementing intelligence authentication schemes that look for just-enough and just-in-time authentication data are ways to provide the access and ease of use customers demand. Authentication is critical to success when it comes to securing your customers' identity data, as well as their financial, personal and confidential information.

Given the wide range of services customers need to access, authentication across all scenarios isn't always easy. A great place to start is to ensure all new services provided to customers follow your defined process process to implement authentication from a centralized service, and working backwards within an application portfolio from there. Of course, ensuring authenticated users only have access to data they properly authorized for is another critical control to have in place, an absence of which has historically resulted in the broad exposure of customer data.

ABOUT PING'S CISO ADVISORY COUNCIL:

Made up of CISOs from leading global enterprises, this group provides insight to Ping Identity on security, privacy and compliance challenges within the global enterprises we serve. It helps inform Ping's strategic vision, product roadmap and go-to-market strategies. Interested in getting involved? Please reach out to your account executive to learn more.

References

[1] Clarke, David and Ron Klinghorn. "Experience is everything; here's how to get it right." PwC. Mar 26, 2018.

[2] Bridges, Tim, Jerome Buvat, Aritra Ghosh, Geert van der Linden and Marisa Slatter. "Cybersecurity: the new source of competitive advantage for retailers." Capgemini. May 9, 2018.