8 THINGS
YOUR C-SUITE SHOULD KNOW ABOUT IDENTITY

By Ping Identity's CISO Advisory Council, comprised of CISOs from 12 enterprise organizations, including: Frank Aiello, CISO for American Red Cross; Diane Ball, CISO for BCBS Tennessee; Steve Martino, CISO for Cisco; Stanton Meyer, CSO for CoBank; Ben Mayrides, CISO for Cvent; Sam Masiello, CISO for Gates Corporation; Larry Whiteside, CISO for Greenway Health; Michael Strong, CISO for GCI; Chris Gullett, VP of Information Security for Allegiant Air; and Adrian Mayers, CISO for Vertafore.

In most enterprises, the senior executives don't fully understand the strategic importance of identity to both security and digital transformation. Given that, Ping Identity invited the Chief Information Security Officers (CISOs) from leading enterprises to identify a top eight list of the things every CxO needs to know about identity.

#1

IDENTITY IS A KEY PART OF SECURITY, AND SECURITY IS A KEY PART OF BUSINESS. We all know that security breaches are bad for business; they can destroy business results and kill a brand. Likewise, poor data governance can be equally bad, especially in the era of General Data Protection Regulation (GDPR). Good security has become a differentiator for modern businesses, and good security requires great identity and access management (IAM). If you look at the org charts for different businesses, you will find the IAM team reporting into different functions or distributed across many lines of business. While ideally we believe that IAM should report into the security team, it's not critical. What's critical is that they work closely together. Make sure the IAM and security teams are closely aligned, and each has a say in how the organization's security and IAM decisions are made.

#2

MULTI-FACTOR AUTHENTICATION (MFA) IS INCREDIBLY IMPORTANT—BUT NOT ALL MFA SOLUTIONS ARE CREATED EQUAL. MFA is one of the easiest and most important things you can do to quickly improve your organization's security. And MFA can be accomplished in many ways. Some ways—like one-time passwords over SMS—are easy to scale and deploy, but also easy for attackers to compromise. Other ways—like Personal Identity Verification cards—are very secure, but a pain for employees to carry and use. Make sure you are choosing the right levels of security and usability for the right people in your organization.

#3

IAM IS FOR EVERYONE. Identity and access management isn't just for your workforce identities. It's for your customer and partner identities too. New regulations like the European Union's GDPR are restricting how companies can collect customer information and what they can do with it. Having good customer and partner identity management and data governance is critical to competing in a global market in the twenty-first century.

#4

IAM MAKES THE USER EXPERIENCE MORE PERSONAL AND COST EFFICIENT. Security teams already know the value of identity and access management, but marketing and product teams are also catching on. A bad login experience can make a customer reluctant to come back to your site after they've bought something, or worse, abandon their transaction before they are finished. A great login experience can make a customer feel like you know them. With IAM, you can remember their preferences across channels and whisk them through checkout with minimal effort.

#5

IDENTITY IS MUCH MORE THAN SINGLE SIGN-ON. Seamless, secure login is critically important, but that's only the beginning of the dividends that identity investments can yield. Usable identity management can make your employees more productive by giving them access to the right tools just in time. It's a huge drain on morale for employees to go through a long, involved process just to get to the resources they need to do their jobs. Good provisioning and access control tools can get them up and running in minutes rather than days—and remove access just as quickly once it's no longer needed. Good data governance can help your customers understand what they've consented to, how you're using their data and how you're protecting their privacy.

#6

EVERY ORGANIZATION NEEDS A "ONE IDENTITY" INITIATIVE. Maybe it's an unachievable goal to have one and only one username for every person who touches your organization throughout their entire life. But it should be an aspiration for every organization. Permissions and access levels can change suddenly. People get hired, they switch positions, they get promoted, they retire. How will your organization make sure that every permission is changed at just the right time if people have multiple usernames to log in to multiple systems? That's a nightmare for both users and administrators. Implement a "one identity" initiative with the goal of solving that problem.

#7

IAM IS AN ENABLER OF INNOVATION AND SPEED. Large organizations are buying or building new applications constantly, and the best ones have implemented internal identity application programming interfaces (APIs). Your development teams should not be building login systems; they should be leveraging centralized identity microservices that can tell them whether their users are logged in and exactly the information they need, right when they need it. Companies without this identity infrastructure will be reinventing the wheel every time they build or buy new software.

#8

IDENTITY IS ESSENTIAL FOR COMPLIANCE. Financial and privacy regulations across the globe, such as Open Banking and Payment Services Directive 2 (PSD2) in Europe, now require companies to prove that they have obtained consent to collect customer data, use it in transactions and act on behalf of customers. This is a core capability of identity management. You have to know that your customer has one and only one account, that they can access it securely and that their data is only available to the people and applications that are allowed to access it. If your organization touches healthcare, education, financial transactions, government services or personally identifiable data, identity can help you reach compliance faster, with complete assurance that you're doing right by your customers.

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.

To learn more about how identity can help you secure your business, improve productivity and provide personalized customer experiences, visit pingidentity.com.

Ping Identity.

#3336 | 07.18 | v02