Deloitte.

IBM Platinum Business Partner

The business of identity

When CMOs and CISOs align, user experience and trust go hand in hand

A new way to look at identity

Are you really who you say you are? The ability to know and understand who's on the other side of an interaction plays a role in the relationship between an organization and the people it serves.

Traditionally, that was implicit, because people did business face to face. Later, instruments like signatures, fingerprints, and eventually digital authenticators became part of engagement—but for a long time, their purpose was purely a matter of verification. Verifying identity meant protecting people, their money, and now their private data.

More recently, marketers have embraced identity for their own purposes. Aided by technology, deep knowledge about a customer or constituent can help refine appeals, deepen relationships, and build loyal behaviors. But many of the ways a Chief Marketing Officer (CMO) uses identity can run the risk of eroding the protective mission that the Chief Information Security Officer (CISO) cares about—the mission that brought identity into the operation in the first place.

CISOs protect the gates and represent the traditional mandate of identity. CMOs strive to reach past them and represent the new possibilities that identity can provide. Both are using the same technology. And both need to be in sync. CMOs and CISOs should learn about each other's operations, communicate more, and build a broad view of identity that serves both missions equally well. Working together is the path forward in today's technology-dominated environment. It can also help the organization realize more benefits from its cyber investments than either of them could alone.

In this joint approach, identity is still vital in keeping systems and data secure. But now it means and does more, both for commercial enterprises that serve customers and for public enterprises that serve constituents. It's a way to more consistently engage customers and constituents—in addition to confirming that you're engaging the correct person in a secure manner.

The place where you meet your customer forms the foundation of trust, and trust is the foundation of a brand.

Together, the CMO and the CISO have a chance to drive more value by taking a fresh look at identity.

The CISO's issue may be that this engagement is also exposure, and that the CMO typically doesn't consult with the CISO before putting it into action. And the CMO's issue? Managed poorly, identity can potentially drive customers away. *(What? Didn't I just sign in?)*

But if the two functions collaborate, identity can be a shared cornerstone. It can be an organization's key to more responsive, personalized interactions—with the nuisance part fading into the background. It can empower the organization to meet people in a consistent way when and where they want those interactions to happen, while structuring those interactions in a way that avoids added risk.

The effects of this change can ripple throughout an organization. In practice, many of them have to do with technology. But perhaps one of the most important ways a company can adapt to this change is through the shared purpose of making engagement easy and intuitive—specifically, by bringing the CISO and CMO into closer contact.

The benefits of effective digital identity management flow both ways. Customers and constituents can find a new experience waiting for them when they no longer have to juggle passwords or squint at Captchas. And when they start receiving truly personalized service, it will feel responsive, not intrusive, in nature. For agencies, the intent is better mission performance. For businesses, the ability to know and follow customers opens new ways to connect with and satisfy them for long-term growth.

What stands in the way? For some, it's the space between two perspectives. If you're a CMO, your knowledge of your customer might be based on personas, segments, relationship length, or buying behavior. To you, identity could be as simple as someone's email address. Meanwhile, if you're a CISO, identity is about security—protecting data and controlling access. Traditionally, if you've satisfied that requirement, the job is done. The truth is, each of you has a chance to drive more value by taking a fresh look at identity. And if you collaborate, you can create a new identity regime that promotes instead of prohibits.

Client interactions seldom involve walking up to a counter anymore. Almost every touch point—be it in person, online, or on the phone—includes a request to share information or register for future interaction. That's why trust, customer experience, emotional connection, and brand value are inseparable now. Identity is important to helping them *work together.*

Cyber comes of age

As a CMO, you can use a new understanding of relationship intelligence to amplify the scope of market research and reactiveness. Consider a customer or constituent who opens an email one day, visits the website a second day, calls a physical location the third day, and uses the mobile app the fourth day. The old approach to identity might have created different access records in different places. When identity works cross-platform, your marketing organization can see and connect those dots to detect a likely interaction, and perhaps push out an alert or offer. None of that is possible if you wait for a member of the public to walk through the door.

And for the CISO? You can also take potential advantage from a new approach to identity. A system that works across channels and touch points has the dual benefit of making an experience less cumbersome and more convenient for the people your organization serves while at the same time making your view of the user more consistent and trackable from one interaction to the next. And whether the user is aware of it or not, the additional protection of a broad approach means more security not only for the organization, but also for the user's information.

Then and now

Personalization is a powerful way to help an organization work better, whether that means growing revenue or executing on a public mission. But it takes real insight: Leading organizations don't just collect data—they use it. Your effort to discover a user's unmet, unexpressed needs can spell the difference between asking for loyalty and earning trust.

Then	Now
Security is there to protect data.	**Security is only one of the values identity can provide.**
Identity is the record you verify to make security work.	**A digital identity is a broadly applicable functionality that helps drive commerce, tie customer behaviors together, and add to trust in the brand.**
The information that makes up identity is there for its own sake, to verify that one key matches another to unlock access.	**The information that makes up identity is a key that opens many doors, not only in security but also in relationship management and customer experience enhancement.**
Identity is something you deal with on your way to interacting with the brand.	**Identity is a central part of how customers experience the brand.**

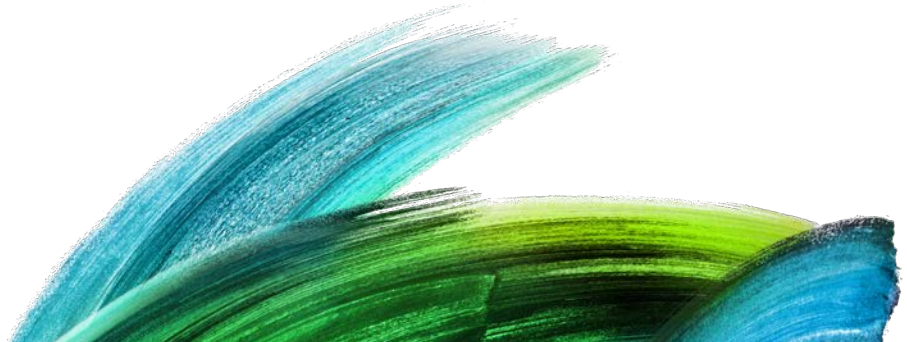
The external view

Comfort and engagement

When you adopt a new vision of digital identity that supports both security and a better user experience, the result can transform what it feels like for someone to do business with you. Smoothing out processes such as logging in and executing transactions is a first step that many will likely welcome, but the change can be more profound than that.

Imagine the user experience of risk-based authentication melting away so that instead of standing out as a separate, intermediate activity, it becomes part of the experiences people came to you for in the first place, such as researching, buying, servicing, or registering. Putting an end to clicking on images with street signs or remembering your first dog's name is only part of the shift. In this vision, there are fewer, if any, visible authentication steps whatsoever.

Combine that with an identity-fueled relationship management system that can apply your preferences across time and platforms, and the result is an experience that can encourage people to interact with you more often and more willingly, whether that means buying and spending or using government services more frequently. Tomorrow's high-tech approach to identity may feel a lot like yesterday's low-tech approach: It won't get in the way.



The enterprise view

Interactions built on trust

We know that company—the one we grew up with, a familiar brand in the households of our childhood. Now it's gone. The wave that broke over so many defunct bookstores, airlines, and car makers is the Fourth Industrial Revolution. If you create a customer-centric organization, as opposed to an organization that "has" customers, you can be among the ones to ride that wave.

A digital experience that uses identity instead of stumbling over it can give you the ability to solidify trust with your customers and inspire them to invest in your brand. This isn't a swap-out of tools. It's a new definition of how to do business with people.

What can spell the difference between the brand that failed and the brand that's writing a new destiny for itself? The ones that failed to keep up may have taken market share for granted, lost the confidence of the people they served, or coasted on a reputation rooted in the past. They may have built a new reputation—for ineffectiveness—or stopped giving people new reasons to trust them.

Operating effectively in the digital world requires organizations to shake loose of the idea that identity and security are the same thing. Everyone talks about putting the customer at the center—and identity is a way to make that more than a slogan.

What can spell the difference between the brand that failed and the brand that's writing a new destiny for itself?

The end of simple decisions

Customer identity used to be a binary matter. Are you who you say you are? Fine, then we'll take a personal check. Now, it's a variable that changes along more than one axis.

Consider levels of security. The traditional "in or out" method might have made it as difficult to buy a fob for your car keys as it was to buy the whole car. Now, a more flexible approach to digital identity may allow a merchant to require one high standard of authentication to authorize a major purchase, but a second, less onerous standard to complete an account inquiry or a minor transaction. That makes doing business more pleasant for the public, and more manageable for you.

Consider methods of authentication. One customer may be comfortable keying in a password—even one with strong criteria such as alphanumeric requirements that others find annoying. The next one is accustomed to letting her thumbprint be her password. Someone else may prefer voice or facial recognition. An identity system that locks into a single methodology will likely end up disappointing someone. But a system that is engineered to be flexible, so each user can find the same ease of experience across a combination of multiple potential techniques, can win their appreciation. It can also be more secure in the end, even though that is no longer the only objective.

When your organization's approach to digital identity follows a person from touch to touch and channel to channel, your ability to use that identity to make sensible, context-based decisions increases.

Bridging the divide

If an organization can't make the leap from one view of identity to another, then this is purely academic. Responsibility for the way identity is approached is probably divided between two people: the CMO and the CISO. How do the two perspectives differ in your organization?

Whether you're the CISO or the CMO, you're likely in a transformative frame of mind these days. For the marketing chief, the transformation is in ways technology and business practices can combine to elevate the customer experience. For the security chief, the transformation is about building security into the ways a business operates instead of putting new fences in front of old structures.

The CISO and the CMO are on different fronts of the same battle, working toward the same goal. Shouldn't you be working together?

Today's reality

Where many CMOs and CISOs are coming from

Chief Marketing Officer (CMO)

- It's my job to protect and extend the brand. Identity helps me do that.
- My customer channels keep accumulating customer information and I'm expected to handle the response when someone breaches it.
- The phantom sales of abandoned digital shopping carts testify to people's disappointment with the user experience we're offering them.
- We keep asking customers to prove we trust them. What are we doing to encourage them to trust us?
- I don't talk to the CISO very often.

Chief Information Security Officer (CISO)

- It's my job to protect the company and its customers from risk—and empower the business. Identity is the foundation of how I get that done.
- I'm consumed with satisfying concerns about compliance, security, and trust, in particular with regard to the new EU General Data Protection Regulation (GDPR).
- My view focuses on my organization's boundaries—controlling who can enter.
- My people are sophisticated technology professionals and we're spending half our manpower budget fielding calls about forgotten passwords.
- Consumers? Business partners? Vendors? That's the business line's problem.
- The business has its timetable. My application development and deployment work has a timetable. Sometimes they coincide.
- I don't talk to the CMO very often.

Tomorrow's potential

Where CMOs and CISOs can go

Chief Marketing Officer (CMO)

When people do business with us, identity is built in, integrated, and transparent. I can focus on my market, and our customers can concentrate on the transactions they want to carry out, without experiencing a barrier.

Finally, the channels and platforms we've invested in can work together and provide additive value because identity doesn't separate them into distinct experiences and data regimes. Omnichannel marketing has "come true at last," and the result is more loyal customers with enhanced lifetime value to my organization.

I have a deeper view into my consumers' preferences and likely actions, so I can anticipate what they want and deploy new offerings right when people are ready for them.

My 360-degree view of the customer base, as a whole and at the individual level, opens up strategic insights I can use to plan more effectively and play a more meaningful role in the organization.

The CISO and I have objectives in common—because user experiences need to be secure and engaging, instead of one or the other.

Chief Information Security Officer (CISO)

Instead of functioning as the internal security force, we have a more direct role in driving the consumer experience, with the stature, budget, and resources to match.

I'm able to offer IT professionals an employment experience that rivals the brand-name tech giants, because the work we do is more varied and meaningful and contributes more visibly to the front-end performance of the enterprise.

Instead of being the ones in charge of saying "no" all the time, my team and I are contributing to the environment of trust that drives the business forward. This changes the way people look at us in the hallway—and in the boardroom.

The CMO and I have plenty to talk about—because we both can benefit when we create user experiences that meet the new dual standard of security and favorability.

Realizing the possible

What CMOs and CISOs should be talking about

Chief Marketing Officer (CMO)

- Are we still making customers satisfy Captchas?
- Do our systems apply identity effectively from one channel to another, or are we duplicating efforts and structures?
- Is identity a part of our brand experience that people value? Or something that stands between them and that experience?
- Are we ready to respond to a breach of private customer information?
- When was the last real conversation I had with the CISO?

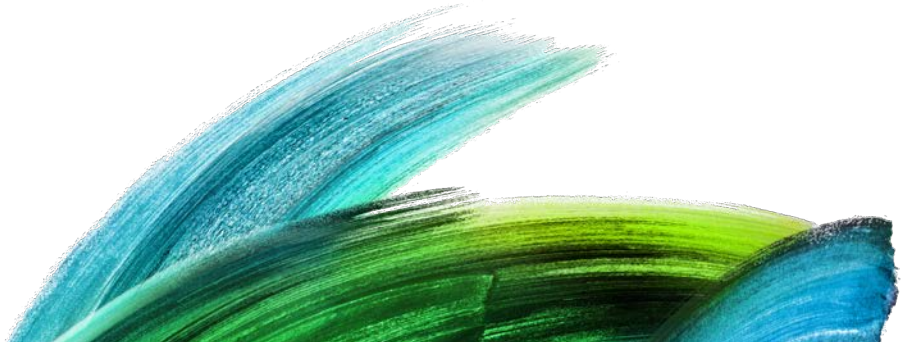
Chief Information Security Officer (CISO)

- Does our organization make identity a less bothersome part of the digital experience?
- Is identity access management a cost center or a source of value?
- Do our efforts to secure the organization get in the way of sales?
- How many times a day do I say “no”?
- When was the last real conversation I had with the CMO?

Deloitte and IBM can help you make it happen

As an important facet of an organization's overall digital transformation, identity transformation is more than just a change in technical safeguards. It extends from core information security, marketing, and constituent service functions to touch areas such as governance, finance, culture, and even business model. Bringing this kind of change to life takes more than just systems implementation.

Through the business experience and global reach of its consulting and advisory practices and the marketing know-how of digital veterans, Deloitte can help you realize the intent of trust-based digital identity and translate it into experience and engagement. And with our understanding of the specialized tools IBM brings to the challenge, you can take advantage of end-to-end solutions that many single-track implementers aren't set up to match.



IBM Platinum Business Partner

For almost 20 years, Deloitte and IBM have helped global enterprises address their toughest business issues. This smarter teaming approach often results in better service and higher value for our joint clients. Our unique alliance unites the depth and breadth of IBM's technology portfolio with Deloitte's practical, innovative solutions. By working together, Deloitte and IBM offer customized solutions focused on the business issues important to you.

We bring a three-stage approach to help you reimagine your approach to digital identity and customer experience.

1

We advise
We help you understand the business problem, we place it in a context of current market trends, and use those insights to develop a strategy that's specific to you.

2

We implement
We combine our own technology solutions and professional experience with IBM's to put effective systems in place.

3

We help operate
We contribute to the operation and enhancement of systems in an iterative way long after the point when others consider a project finished.

IBM is a critical part of this equation. Its leading engagement and security tools are engines that combine with Deloitte's advisory and implementation capabilities to arm you with a trusted end-to-end solution. Our accelerators also differentiate us through a track record of performance and improvement.

Harmony in the C-Suite, happier customers

Identity and security are no longer just synonyms for the same thing. True, identity is still a visible part of the user experience. But leading organizations can make it visible in more than one way: not only as a safeguard for access and data, but also as the foundation of a truly personalized experience they can enjoy more. CMOs and CISOs can drive that change—by consulting each other about decisions that affect the customer's experience.

The old challenge was a tension between protecting the company and welcoming people across the threshold. The new reality is that those two aims don't have to be in tension anymore. An effective and pleasant user experience can make people more willing to build a relationship with you, while enhancing the control of fraud and risk that led many to set up their digital front doors in the first place.

It's time for public-facing enterprises to catch up to the evolution that cyber has already achieved—to join the era of maturity and ubiquity and give each user an experience that follows them across channels, devices, and interaction types. The first step is to work toward a feeling of frictionless engagement from the user's point of view.

If you follow different agendas as the CMO and the CISO, draw on different resource plans, and keep company with your own siloed teams, your organization may move toward a more effective control regime. Or it may move toward a more effective end-user experience. But not both.

When you realize your two functions are on the same mission, your agendas, resources, and decisions can mesh.

Start talking

The goal is a smooth-flowing experience that both the enterprise and the people it serves can enjoy. That's an easy vision to articulate, and a difficult one to make real. Part of achieving that goal will be technical. But the first step is to talk.

Not only with Deloitte and IBM, but also with each other. Your enterprise exists because of what it's good at—something it makes, something it does. Until now, identity has typically has stood between your customers and that specialty. Working together, the CMO and the CISO can usher in a new approach that takes identity out of the way. The people are ready. *Are you?*

Apurva Pangam
Principal
Customer and Marketing
Deloitte Consulting LLP
apangam@deloitte.com

Daniel Poliquin
Principal
Risk and Financial Advisory
Deloitte & Touche LLP
dpoliquin@deloitte.com

Ash Raghavan
Principal
Risk and Financial Advisory
Deloitte & Touche LLP
araghavan@deloitte.com

Nick Thompson
Senior Manager
Customer and Marketing
Deloitte Consulting LLP
nthompson@deloitte.com

Deloitte.