Deloitte.
Insights

FEATURE

Rediscovering your identity

How a comprehensive approach to digital identity management can empower everyone

Michael Wyatt, David Mapgaonkar, and David Jarvis

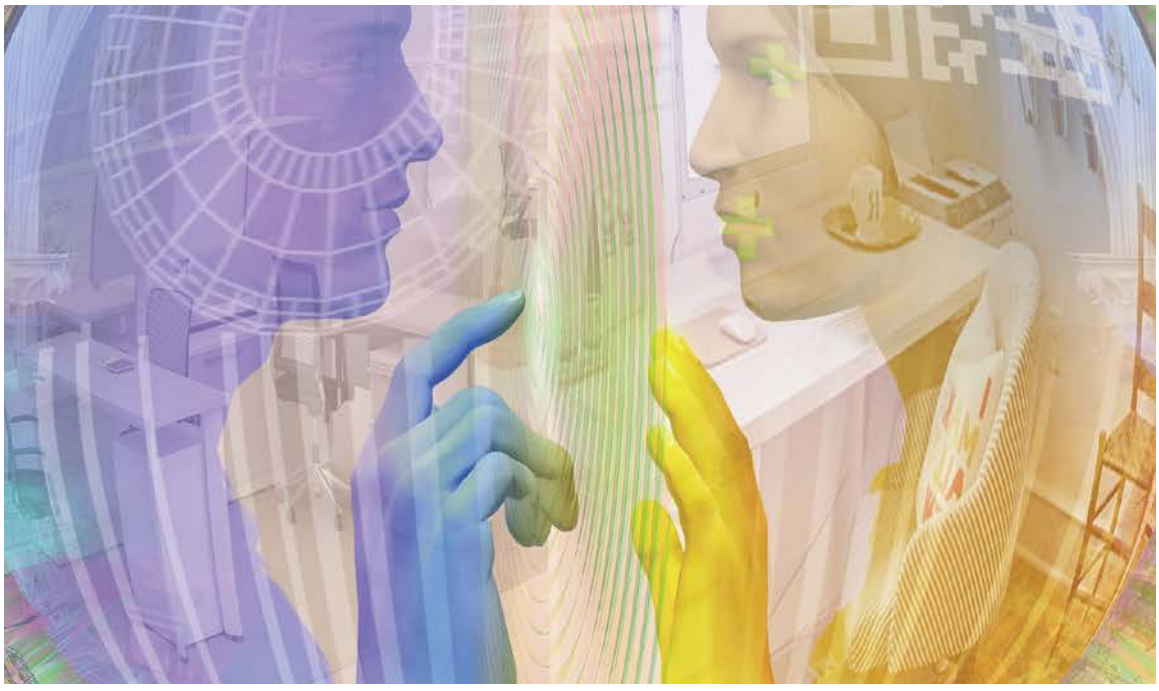
A REPORT BY THE DELOITTE CENTER FOR TECHNOLOGY, MEDIA & TELECOMMUNICATIONS

With traditional digital walls gone and consumer expectations rising, companies are struggling to find effective digital identity management solutions. It is critical to approach enterprise and consumer identity with equal vigor, explore managed services, and integrate new technologies.

FROM WAX SEALS and stamps to passports and fingerprints to biometrics and behavioral analysis—humans have always looked for foolproof ways to validate that those they deal with are who they claim to be and can be *trusted*. In these times of increased concern over data breaches, fraud, and privacy, trust is paramount. And in our digital society, trust is determined through *digital identity*—the corpus of data about an individual, an object, or an organization that helps identify them through unique qualities and use patterns.

Effective digital identity practices are more important to business success than ever. They are vital for presenting a compelling first contact point to customers, protecting sensitive data, enabling secure transactions, and transforming business processes. They can enable new ways to engage with consumers via social media, improve collaboration within the enterprise, and automate and simplify cybersecurity practices.

Breakdown of digital walls, changing user expectations, and emerging technologies are giving rise to a digital identity crisis of sorts.



However, companies are having to deal with increasing challenges in enterprise and consumer identity management. One of the reasons for this is the breakdown of traditional digital walls, which has blurred the distinction between the inside and outside of an organization. This shift, along with changing user expectations, emerging technologies, a shift to cloud-based services, growing business needs, and evolving privacy regulations, is giving rise to a digital identity crisis of sorts.

Companies should reexamine, and rapidly evolve, their digital identity strategies—internally, for their enterprise, and externally, for consumers. Only by looking at digital identity management *holistically* and approaching both enterprise and consumer identities with a similar philosophy can organizations get the outcomes they desire. In this article, we take you through a unified strategy to help improve digital identity practices across the organization.

Digital identity management: The challenges

There are many emerging trends and challenges shaping the evolution and management of digital identity—both enterprise and consumer. Our research revealed some of the top ones:

Digital identity management can be overshadowed by more urgent concerns. It is not that companies don't think it is important—they may be dealing with other pressing cybersecurity issues. They also may need to show immediate progress and return on investment on cybersecurity initiatives. However, it takes some patience to implement digital identity projects as they tend to be more of a marathon than a sprint. This challenge shows up in how much time and money companies are spending on the problem. In Deloitte's *2019 Future of cyber survey*, which surveyed 500 C-level executives responsible for cybersecurity, more than half of the respondents (54 percent) said they dedicated 10 percent or less of their cyber budget to identity solutions, with 95 percent committing 20 percent or less. Additionally, 88 percent of all respondents spend 10 percent or less of their time on identity and access management.[1]

Companies are wary of outsourcing identity management. Most cybersecurity leaders are protective of their systems and hesitant to let others manage them. According to Deloitte's *2019 Future of cyber survey*, the top preferred way to procure, implement, and provide ongoing delivery of identity capabilities is on-premise implementations, with 36 percent of respondents selecting this option. This is especially true of chief information security officers (CISOs), with 60 percent preferring on-premise solutions. Cloud-based identity-as-a-service (IDaaS) implementations were selected by just 24 percent of all respondents, and only 32 percent outsource their identity and access management to third parties.

Why this reluctance? The CISO of a major telecommunications company explains, "I have had applications that are many years—if not decades—old; a lot of in-house, homegrown applications that none of the cloud providers could easily integrate without making changes to their cloud infrastructure."[2] Such worries about integration, flexibility, getting specialized support, and a lack of faith in available capabilities are quite reasonable and likely hold back companies from opting for IDaaS.

Rising global data privacy regulations pose compliance challenges. Governments across the world are exploring—and implementing—new legislation and regulations to protect personal data privacy and digital identity. Executives and cybersecurity leaders have to address mandates such as the EU's General Data Protection

Regulation (GDPR), the California Consumer Privacy Act (CCPA), and Canada's updated Personal Information Protection and Electronic Documents Act (PIPEDA). They also are expected to follow many other guidelines including the Cybersecurity Framework from the National Institute of Standards and Technology (NIST).[3] This increases the burden on cybersecurity leaders and executives as they're required to develop a more comprehensive view of their consumers to comply with legal and audit-related mandates.

Some companies have moved their identity stacks to the cloud and others are consuming identity-as-a-service.

A steady shift toward managed services and AI

Challenges aside, approaches to digital identity management are starting to change quickly. Organizations are increasingly living in cloud-centric environments and there is a general shift to managed services and consumption-based models. Deloitte's 2018 study, *Accelerating agility with everything-as-a-service*, found evidence of this shift.[4] Seventy-one percent of companies report that as-a-service (XaaS) now makes up more than half of their organization's enterprise IT (with the remainder being traditional, nonservice-based IT).

As part of this shift, some companies have moved their identity stacks to the cloud and others are consuming identity-as-a-service. Gartner says that by 2022, "Forty percent of global midsize and larger enterprises will use identity and access management as a service (IDaaS) capabilities to fulfill most of their identity and access management (IAM) needs, which is up from 5 percent today."[5] One of the reasons for this is that cloud providers and third-party cloud operators are likely to have much more sophisticated capabilities than what a company may have in-house, which eliminates the need for updates and upgrades to both software and infrastructure. Also, with many companies facing a shortage of skilled cybersecurity professionals, using managed services helps eliminate the need to attract, train, and/or retain this hard-to-find talent.

Many organizations are also experimenting with and integrating a number of new technologies to improve their digital identity capabilities. Moving beyond simple logins and passwords, they're increasingly using advanced authentication methods such as physical biometrics and behavioral monitoring as standard practices in digital identity management. In today's "zero trust" environment, companies continuously monitor and authenticate users—constantly determining their level of risk based on who they are, what they access, and when and where they do it. To facilitate this, they are increasingly turning to AI technologies that help them automatically detect anomalies and identify behavior that doesn't fit a particular pattern. Twenty percent of respondents from Deloitte's *2019 Future of cyber survey* are prioritizing AI-driven threat identification and assessment as a transformational capability in digital identity management.

In today's "zero trust" environment, organizations have to continuously monitor and authenticate users to determine their level of risk.

However, there are mixed opinions on the use and maturity of AI in identity management. A CEO of a US-based cybersecurity and risk advisory company is optimistic about AI, and says, "AI or machine learning is going to be a capability that's associated with risk assessment—not just identifying the user but also identifying the device and the health of that device, whether that's been compromised or not. It has to be more than just ID and authentication."[6] On the more pragmatic side, Alex Beigelman, chairman of the National Cybersecurity Society, says, "The authentic stuff is very much in its infancy. It is being used, but in limited ways and only by a limited number of companies that have the resources to do some experimentation and take some risks."[7]

Two sides of the same coin: Consumer and enterprise identity

While reexamining their digital identity management strategies, organizations should think about challenges related to *both* consumer and enterprise identity management to understand what they can do to create a holistic approach. There are different business requirements, technical approaches, and challenges for each, but there are sound fundamental practices that can be applied to both. Let's look at some of the unique challenges:

CONSUMERS ARE EXPECTING MORE

With the increasing depth and complexity of digital interactions between consumers and businesses, attention to consumer identity management has increased commensurately. Companies want to ensure that those logging in are who they say they are and that they are having a good experience. The reasons for this are many, including:

- Consumers expect more; they want to log in just once and get quick access to what they need, when they need it.
- They are more connected than ever before and want a consistent experience across the multiple channels they engage with—call centers, mobile, Web, chatbots, and virtual assistants.
- They are increasingly informed and concerned about privacy issues and hesitant to share too much personal information; they want personalization, ease, and flexibility in their interactions.
- Consumers have come to expect a certain level of visible security. For example, multifactor authentication (MFA) while carrying out online banking transactions makes them feel secure.

Organizations must think about challenges related to both consumer and enterprise identity management for a holistic solution.

Within organizations, the complexity around consumer identity management has increased as well. Responsibility and ownership are often distributed among multiple executives, teams (marketing, sales, cybersecurity, etc.), and IT systems, making coordination of large-scale projects challenging. According to Deloitte's *2019 Future of cyber survey*, companies are focused on many different client- and vendor-facing identity initiatives. The top areas are consumer identity and access management at 28 percent, advanced authentication including MFA at 27 percent, and GDPR enablement/privacy compliance at 25 percent.

ENTERPRISES ARE DEALING WITH MORE

As the pace of business increases and the demands of transformational initiatives multiply, companies shouldn't neglect enterprise identity management either. One of the biggest identity-related problems faced by companies is privilege misuse and compromised credentials, which are used by bad actors and cybercriminals to breach networks. A recent survey commissioned by Centrify covering 1,000 IT decision-makers in the United States and the United Kingdom found that 74 percent of respondents whose organizations have been breached acknowledge it involved access to a privileged account.[8]

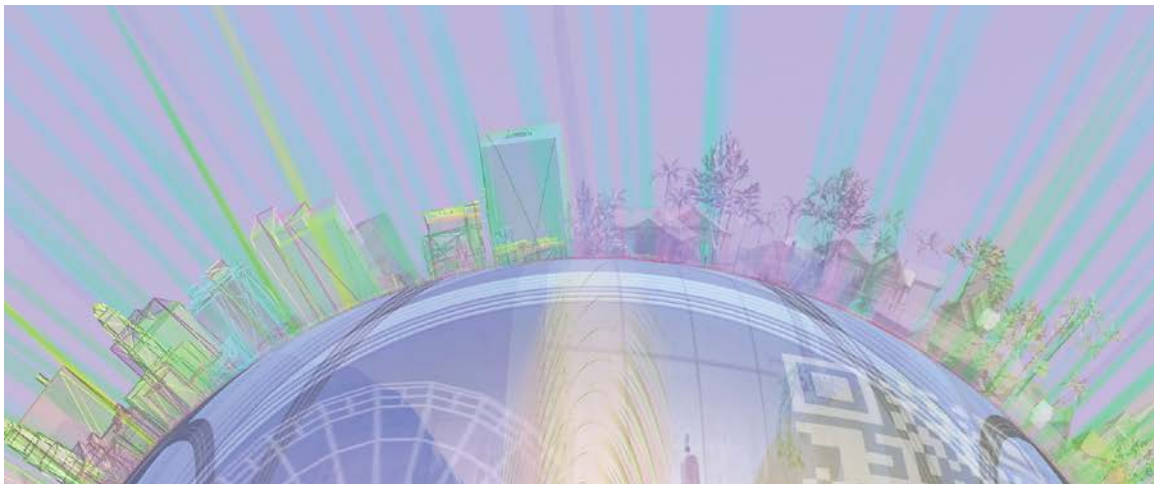
Apart from external threats, companies face a host of internal enterprise identity management problems as well, including the following:

- There continues to be a pronounced shortage of cybersecurity talent, and digital identity typically doesn't garner a large share of focus or spending, so the necessary resources can be scarce.
- Cybersecurity teams have to deal with legacy IT environments and a resistance to migrate to cloud-first architectures. Many haven't built modern systems that are API-based, orchestrated, and enable easy integration with apps.
- There is a rising expectation that cybersecurity can help enable digital transformation and innovation.

The top enterprise identity cybersecurity initiatives, as revealed in Deloitte's *2019 Future of cyber survey*, were advanced authentication (including MFA and risk-based authentication) and privileged access management (PAM)—each selected by 19 percent of respondents.

To fully address these issues, organizations should strive for digital identity management systems that embody a set of common qualities for both enterprise and consumer users (see the sidebar, "A proper digital identity management system should be").

Apart from external threats, companies face a host of internal enterprise identity management problems as well.



A PROPER DIGITAL IDENTITY MANAGEMENT SYSTEM SHOULD BE:

Safe	To ensure security, privacy, and compliance.
Flexible	To work across multiple platforms (on-premise and cloud); work with people, systems, and devices.
Agile	To quickly adapt to changing end-user needs, IT requirements, and new applications.
Scalable	To address the shifting requirements of the business—such as adding new users from an acquisition or managing an influx of customers.
Open	To accommodate many types of users, including employees, consumers, partners, and contractors.
Private	To give users control over their information and an understanding of how it is used and how they can access it.
Frictionless	To provide a seamless and convenient experience for both users and cybersecurity administrators.
Resilient	To overcome potential service disruptions, technology failures, or cyber threats—whether on-premise or in the cloud.

A holistic solution to digital identity management

Considering how deeply enterprise and consumer identities are interlinked, companies should approach both in a similar and coordinated manner to unlock benefits for the enterprise as well as consumers. It is not a question of either/or anymore—a strong, holistic approach to digital identity management can help drive the business, make life easier for cybersecurity teams, and provide superior experiences for both consumers and employees (see the sidebar, "How a holistic approach to digital identity helps").

In the era of cyber everywhere, the operating environment for identity management will likely become increasingly complex—with greater business expectations to meet, new technologies to integrate, multiple data privacy regulations to adhere to, and increasing numbers of people and devices to manage. To navigate this complex environment, there are five things cybersecurity leaders can do to better integrate their digital identity management strategies, processes, and systems into the business:

1. **Pursue a holistic approach to identity:** Treat everyone and everything equally—whether it be a consumer or an employee, a person, a device, or an application. Neglecting a single element of the identity ecosystem could impact the speed at which an organization innovates and operates. Look for cross-pollination opportunities between enterprise and consumer identity management and ways to use your traditional capabilities in new ways.
2. **Help consolidate, coordinate, and align responsibilities:** Identity, data privacy, and regulatory compliance are increasingly overlapping. This means that technology, cybersecurity, legal, and business leaders are all stakeholders in effective identity management, each with their own challenges and ambitions related to user experience, system availability, resilience, risk management, and consumer engagement. Those responsible for identity

HOW A HOLISTIC APPROACH TO DIGITAL IDENTITY HELPS:

Consumers and employees	Cybersecurity teams	Business leaders
Employees can access information they need securely, conveniently—anytime and anywhere. This can support better communication and collaboration and **boost productivity**. Consumers can feel confident and secure in their interactions with businesses, potentially sharing more and creating **deeper relationships**.	Increasing the level of automation in identity management systems through AI can enable cybersecurity personnel to **focus on higher-value tasks** that they don't have time for today and **reduce the chance of human error**. Providing cybersecurity leaders with identity systems that provide a greater level of resilience and control and that continuously monitor user behavior can **reduce organizational risk**.	Being mindful of how the organization asks for personal information and providing options to consumers can **build trust and brand loyalty**—enabling businesses to tailor their products and offerings. Consolidating and automating systems can **reduce costs** and improve operational efficiency and response speed—such as when managing audits, empowering users to perform self-service tasks, and responding to regulatory requirements.

management are in a unique position to inform and influence conversations and decisions and can ensure that the organization adapts more quickly.

3. **Advocate an outcome-based approach:** To empower innovation efforts and drive digital transformation, look at making identity a service for the entire organization. Identify business outcomes—such as improving consumer retention or streamlining HR processes—that identity management can help with. To help overcome resource constraints, support larger transformational projects focused on these greater outcomes.

4. **Explore managed services:** Given the array of resource and talent challenges and cybersecurity issues, look for help to address your business outcomes. If your organization can't commit the required resources to identity management, explore third-party managed services, either on-premise or in the cloud. They can offer the latest skills and capabilities, increase automation, and future-proof identity systems. The shift might not be possible for all, and there may be resistance to giving up some control, but don't disregard the option. To address concerns, consider taking a phased approach.

5. **Prepare to become AI-enabled:** AI technologies such as machine learning are becoming integrated into many identity management solutions—from automated account concierges to fraud detection. Explore what their adoption may mean for your digital identity capabilities. What outcomes are you looking for—to automate or optimize existing processes or to create entirely new capabilities for authentication and risk assessment? How will it impact how your cybersecurity team spends its time and what kind of training will it require?

A 360-degree digital identity strategy, built with the above practices in mind, can unlock significant benefits for consumers and employees, cybersecurity teams, and business leaders. Most of all, a unified approach can help build trust and ensure privacy and security, thereby preventing a digital identity crisis. Digital identity systems used

to require a choice between security or convenience—but now you can have both. Be thoughtful about how you design your systems in order to protect assets and avoid being too onerous for employees and consumers. Keep sight of this and the recommendations above as you walk the path of digital identity transformation.

IDENTITY MANAGEMENT FOR TECHNOLOGY, MEDIA AND ENTERTAINMENT, AND TELCO COMPANIES

Every company has a different set of digital identity challenges and a unique approach to identity management. Technology companies, for instance, should be very flexible with their digital identity strategies and systems so they can navigate a fast-moving market. Media and entertainment companies often deal with large numbers of transient customers. Telco companies may have very old systems that are difficult to update or replace and can't integrate easily with modern identity management solutions. However, there are some common factors they should keep in mind while enhancing their digital identity management capabilities. Here are some of them:

- **They have been minimally regulated compared to other industries.** This means that they don't necessarily *have* to do certain things with respect to digital identity that other companies are required to do. If they do them, it is because they are the *right* things to do for customers and employees and help maintain trust and security. A lack of regulatory pressure can potentially slow digital identity transformation. This is beginning to change with the advent of new regulations such as the GDPR and the CCPA, which are making it necessary for less experienced industries to change their approach.
- **They have a high level of technical expertise and experience.** Many technology, media and entertainment, and telco companies employ highly skilled engineers and technologists and may feel they can handle any digital identity problem that comes their way; that they can just build what they need from scratch and move on to the next problem. However, a proper digital identity approach weaves together many complex systems that require specialized skills and constant vigilance. Companies should focus high-end technical talent on their core mission and leverage mature identity solutions already available.
- **They face greater potential consequences for mistakes.** Many of these companies create the products and services that underlie and power all other industries. If a breach were to occur in one of them due to mismanaged credentials, the public and market reaction may be disproportionately larger than if it happened to a retailer or industrial company. This makes a comprehensive digital identity strategy and approach even more essential.

Endnotes

1. Deloitte, *2019 Future of cyber survey*, 2019. The survey was conducted by Wakefield Research among 500 C-level executives who oversee cybersecurity at companies with US$500 million or more in annual revenue (100 CISOs, 100 CSOs, 100 CTOs, 100 CIOs, and 100 CROs) between January 9 and 25, 2019, using an online survey.
2. CISO of a telecommunications company, interview with authors, August 16, 2019.
3. NIST, "Cybersecurity framework," accessed October 23, 2019.
4. Gillian Crossan et al., *Accelerating agility with everything-as-a-service: IT providers are shifting from traditional models to XaaS flexible consumption models*, Deloitte Insights, September 17, 2018.
5. Gartner, "Gartner predicts increased adoption of mobile-centric biometric authentication and SaaS-delivered IAM," press release, February 6, 2019.
6. CEO of a US-based cybersecurity and risk advisory company, interview with authors, August 28, 2019.
7. Alex Beigelman (chairman, National Cybersecurity Society), interview with authors, August 27, 2019.
8. Centrify, "SURVEY: Privileged access management in the modern threatscape," accessed October 23, 2019.

Acknowledgments

The authors would like to thank **Shreyas Waikar**, **Prakriti Singhania**, **Naresh Persaud**, **Alex Bolante**, **Anthony Berg**, **Nicole Hockin**, and **Hillary Campbell** for their contributions to this report.

About the authors

Michael Wyatt | miwyatt@deloitte.com

Michael Wyatt is the Deloitte Risk and Financial Advisory principal for the Cyber Risk Identity practice at Deloitte & Touche LLP. He is a recognized leader in identity management as well as state government cybersecurity and privacy approaches with a deep focus on identity management, breach remediation, and statewide security assessments and security program development. Wyatt is the Deloitte Risk and Financial Advisory leader for the State of Texas and the State of South Carolina and delivers cybersecurity services to Georgia, Virginia, and several commercial clients. Connect with him on LinkedIn at www.linkedin.com/in/mikewyatt/ and Twitter @michaelswyatt.

David Mapgaonkar | dmapgaonkar@deloitte.com

David Mapgaonkar is a principal in the Cyber Risk practice at Deloitte & Touche LLP. He is the US Technology, Media & Telecommunications industry leader for the Cyber Risk practice and also leads the Privilege Access Management offering within the Cyber Risk Identity practice. Over his 20 years of experience, he has led dozens of cyber risk engagements for Fortune 500 clients, ranging from strategy to technology implementation to managed services and operations. In addition, Mapgaonkar serves as the Deloitte Risk and Financial Advisory leader for Twitter and Salesforce and delivers cybersecurity services to Hewlett Packard, Uber, Airbnb, F5 Networks, and several other clients. Connect with him on LinkedIn at www.linkedin.com/in/david-mapgaonkar-7a428/ and Twitter @davidmapgaonkar.

David Jarvis | davjarvis@deloitte.com

David Jarvis is a senior research manager in Deloitte's Center for Technology, Media & Telecommunications, Deloitte Services LP. He researches and writes about a wide variety of emerging business and technology topics, including cybersecurity and artificial intelligence. He has more than 14 years of experience in the technology industry and is a passionate expert and educator focused on uncovering strategic insights to help leaders manage for the long term. Connect with him on LinkedIn at www.linkedin.com/in/davidajarvis and Twitter @dajarvis.

Contact us

Our insights can help you take advantage of change. If you're looking for fresh ideas to address your challenges, we should talk.

Industry leadership

Michael Wyatt
Identity leader | Principal |Deloitte & Touche LLP
+ 1 512 227 4171 | miwyatt@deloitte.com

David Mapgaonkar
Leader, Cyber Risk Services for Technology, Media & Telecommunications and Privilege Access Management | Principal | Deloitte & Touche LLP | + 1 408 704 4481 | dmapgaonkar@deloitte.com

Alex Bolante
Consumer identity | Managing director | Deloitte & Touche LLP
+1 619 237 6574 | abolante@deloitte.com

Anthony Berg
Digital identity | Principal | Deloitte & Touche LLP
+1 404 395 6340 | antberg@deloitte.com

About the Deloitte Center for Technology, Media & Telecommunications

In a world where speed, agility, and the ability to spot hidden opportunities can separate leaders from laggards, delay is not an option. Deloitte's Center for Technology, Media & Telecommunications helps organizations detect risks, understand trends, navigate tough choices, and make wise moves.

While adopting new technologies and business models normally carries risk, our research helps clients take smart risks and avoid the pitfalls of following the herd—or sitting on the sidelines. We cut through the clutter to help businesses drive technology innovation and uncover sustainable business value. Armed with the center's research, TMT leaders can efficiently explore options, evaluate opportunities, and determine whether it's advantageous to build, buy, borrow, or partner to attain new capabilities.

The center is backed by Deloitte LLP's breadth and depth of knowledge—and by its practical TMT industry experience. Our TMT-specific insights, and world-class capabilities help clients solve the complex challenges our research explores.

ABOUT DELOITTE CYBER

As a recognized leader in cybersecurity consulting, Deloitte Cyber includes thousands of dedicated cyber professionals, across 20 industry sectors, who help clients better align cyber risk strategy and investments with strategic business priorities, improve threat awareness and visibility, and strengthen their ability to thrive in the face of cyber incidents. The ubiquity of cyber drives the scope of our services. Deloitte Cyber advises, implements, and manages solutions in strategy, defense, and response; data security; application security; infrastructure security; and identity management. In 2019, Deloitte Cyber opened the Cybersphere, a state-of-the-art destination to help clients address their most pressing cyber challenges. The Cybersphere offers a Watch Floor for 24/7 threat monitoring and reconnaissance to help clients detect and respond to threats in real time; a Cyber IoT Studio, where next-generation security is developed and tested; and a client-centered Core, featuring labs that provide disruptive, interactive experiences customized to increases capability and confidence in the face of ever-evolving cyber threats.

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors
Editorial: Prakriti Singhania, Abrar Khan, Anya George Tharakan, and Preetha Devan
Creative: Sonya Vasilieff
Promotion: Hannah Rapp
Cover artwork: J. F. Podevin