Deloitte.
Insights

Tech Trends 2022

Trending the trends: Thirteen years of research

TABLE OF CONTENTS

4 Letter from the editors

6 Executive summary

10 Data-sharing made easy

28 Cloud goes vertical

41 Blockchain: Ready for business

60 IT, disrupt thyself: Automating at scale

78 Cyber AI: Real defense

99 The tech stack goes physical

119 Field notes from the future

131 Acknowledgments

Letter from the editors

Over the past two years, the world has been reeling from the shock of the pandemic, and we are now collectively trying to navigate to our "next normal." Those of us on the *Tech Trends* team believe that this represents the opportunity to engineer a better future—not to just repave the old cow paths of IT but also to rethink how we can all move forward together.

And make no mistake: Moving forward will require every one of us. The best art speaks to the human condition, and the best journalism gives voice to public concerns. There's no doubt the public has been concerned about the rise of "robot overlords," which is why we've all seen plenty of coverage of the topic. In truth, our AI-assisted future is not a dark mirror, nor is it a glib panacea. Seen from the ground, the reality is that organizations are automating soul-crushingly repetitive tasks, freeing humans to focus on more interesting, higher-value problems. If anything, humans are only becoming more precious to their employers. The battle for talent, especially in tech, has never been fiercer.

In this year's *Tech Trends* report, we examine different ways pioneering enterprises are automating, abstracting, and outsourcing their business processes to increasingly powerful tech tools. In doing so, they are arming their employees with superpowers to tackle innovative projects that deliver competitive differentiation. For example, blockchain is enabling organizations to automate processes that occur between third parties, eliminating the need for manual data exchanges, data entry, and reporting—creating an environment where recording *is* reporting. IT departments are automating large segments of their core system infrastructure, allowing precious engineers to get back to actual engineering. And AI is acting as a force multiplier in cybersecurity, detecting and responding to threats automatically and easing the burden on cybersecurity workers.

Of course, the pandemic has fueled this year's trends, but it would be a mistake to view them as a direct response to COVID-19 disruption. Rather than reorienting businesses' goals, the pandemic has simply put an exclamation mark on existing priorities. Enterprises once viewed the types of initiatives we spotlight as projects that would play out over the next five to 10 years. The reality? These trends

need to be tackled today. Customers expect outstanding digital + physical experiences. Workers expect to work anywhere. And your competitors? Your traditional competitors are becoming ever more efficient, and emergent competitors—those with no business being in your business—would be delighted to put you out of business. Digital disruptors don't win because they're small. They win because their lean statures allow them to be decisive, agile, and resilient. To thrive in today's environment, established incumbents are beginning to recognize that thinking bigger requires that they act smaller. *That's* why they're looking to automation, abstraction, and outsourcing, and, in turn, the technology pieces that support those concepts, such as cloud, security, and data.

The pandemic challenged orthodoxies as to what can be accomplished. It showed us how much we can achieve when impediments to productivity are removed and workers are empowered to focus. In IT, workers responded by moving mountains to set up remote work infrastructure and support new ways of reaching customers. This gave IT enhanced credibility. Now, enterprises are looking to their tech teams to drive the next round of innovation: to discover the mountains beyond and move those, too.

At the same time, technology teams find themselves in a precarious spot. Few IT managers would say they have all the people they need. Therefore, in a world of unbounded ambition and finite resources, businesses are trying to figure out how to do more with less.

Tech Trends 2022 chronicles automation as the emerging key to both sustaining and enhancing baseline operations, and how this, in turn, empowers workers to move up the value chain and spend their time solving ever-more-valuable problems.

The future is human. So let's get to work.

Nuno Carvalho
Technology Consulting Partner
ncarvalho@deloitte.pt
(+351) 210 422 500

Rui Vaz
Technology Consulting Partner
ruivaz@deloitte.pt
(+351) 210 422 500

Executive summary

Case studies, insights, and the trends

Data-sharing made easy

- CVS Health
- Catena-X
- DARPA
- Kyle Rourke, Snowflake

Cloud goes vertical

- Marijan Nedic, SAP

Blockchain: Ready for business

- Caisse des Dépôts
- Chow Tai Fook
- US Department of Treasury
- Andre Luckow, PhD, BMW Group

IT, disrupt thyself: Automating at scale

- Capital One
- UiPath
- Anthem
- Bill McDermott and C.J. Desai, ServiceNow

Cyber AI: Real defense

- Sapper Labs Cyber Solutions
- Mike Chapple, University of Notre Dame
- Adam Nucci, US Army

The tech stack goes physical

- Southwest Airlines
- Southern California Edison
- Sheba Medical Center
- Brad Chedister, DEFENSEWERX

Field notes from the future

- Mike Bechtel, Deloitte

Data-sharing made easy

A host of new technologies promise to simplify the mechanics of data-sharing across and between organizations while preserving the veil of privacy. As part of a growing trend, organizations are unlocking more value from their own sensitive data while leveraging enormous volumes of externally sourced data that has traditionally been off limits. This can open a new arena of data-driven opportunities. Indeed, the ability to share secured data with others within an ecosystem or value chain is giving rise to new business models and products. For example, by pooling clinical data on shared platforms in the early days of the COVID-19 pandemic, researchers, medical authorities, and drug makers were able to accelerate the development of treatments and vaccines. Moreover, these same data-sharing protocols have helped drug makers, government agencies, hospitals, and pharmacies coordinate and execute expansive vaccination programs that prioritize efficiency and safety while preserving intellectual property.

Cloud goes vertical

The center of gravity around digital transformation has shifted from meeting the IT needs of an industry-agnostic organization to meeting the unique strategic and operational needs of each sector and even subsector. Hyperscalers and SaaS vendors are working with global system integrators and clients to provide modularized, vertical-specific business services and accelerators that can be easily adopted and built upon for unique differentiation. As this trend gains momentum, deploying applications will become a process of assembly rather than creation—a shift that could reorder the entire value stack. Business processes will become strategic commodities to be purchased, freeing organizations to focus precious development resources on critical areas of strategy and competitive differentiation.

Blockchain: Ready for business

Trendy cryptocurrencies and nonfungible tokens (NFTs) capture media headlines and the public imagination, but these and other blockchain and distributed ledger technologies (DLTs) are also making waves in the enterprise. In fact, blockchain and DLT platforms have crossed the disillusionment trough of the hype cycle and are well on their way to driving real productivity. They are fundamentally changing the nature of doing business across organizational boundaries and helping companies reimagine how they make and manage identity, data, brand, provenance, professional certifications, copyrights, and other tangible and digital assets. Emerging technical advancements and regulatory standards, especially in nonpublic networks and platforms, are helping drive enterprise adoption beyond financial services organizations. As enterprises get comfortable with blockchain and DLT, creative use cases are cropping up in many industries, with established industry leaders expanding their portfolios and creating new value streams, while startups dream up exciting new business models.

IT, disrupt thyself: Automating at scale

Faced with creeping technological complexity and higher expectations of stability and availability, some CIOs are radically reengineering their IT organizations. How? By taking a page from the cloud provider's playbook. They are identifying repetitive, manual processes and applying a combination of engineering, automation, and self-service. The net result is streamlined timelines, accelerated value delivery, and more effective and stable IT across the board. This kind of disruptive automation represents a vast yet underrealized opportunity. Previous technology trends such as NoOps, Zero trust, and DevSecOps share a common theme—the importance of moving to code across the organization. Migrating away from manual administration to engineering and automation, organizations can manage complex systems more effectively and improve the customer experience through improved availability and resilience.

Cyber AI: Real defense

Security teams may soon be overwhelmed by the sheer volume, sophistication, and difficulty of detecting cyberattacks. Enterprise attack surfaces are expanding exponentially. The use of 5G is growing, along with the number of network-connected devices; remote work is gaining ground; and third-party attacks have become increasingly pernicious. It's time to call for AI backup. Cyber AI can be a force multiplier that enables organizations not only to respond faster than their attackers can move but also to anticipate these moves and act in advance. AI can be expanded beyond established applications, such as using it to accelerate data analysis, identify anomalies, and detect threats. These emerging AI techniques can help human analysts focus on prevention and remediation, and developing a more proactive, resilient security posture. And as AI is adopted across the business, it can also be leveraged to help protect valuable AI resources and combat AI-powered attacks.

The tech stack goes physical

With the explosion of "smart devices" and the increased automation of physical tasks, IT's remit is growing again, extending beyond laptops and phones. CIOs must now consider how to onboard, manage, maintain, and secure such business-critical physical assets as smart factory equipment, automated cooking robots, inspection drones, health monitors, and countless others. Because outages could be business- or life-threatening, devices in the evolving physical tech stack require the highest levels of system uptime and resilience. And a fresh approach to device governance and oversight may be needed to help IT manage unfamiliar standards, regulatory bodies, and liability and ethics concerns. Finally, CIOs likely will need to consider how to procure needed technology talent and reskill the current workforce.

Field notes from the future

A bold, technologically sophisticated future awaits—this we know. Yet from our vantage point today, we cannot discern precisely what this bold future looks like, or how we can prosper in it. How can we plan for events that are likely, yet vaguely defined? In *Field notes from the future*, our final chapter of *Tech Trends 2022*, we examine the trajectories of three technologies that will likely dominate the digital landscape a decade or more from now: quantum, exponential intelligence, and ambient experience. Though currently nascent, each of these technologies has captured the imagination of researchers and the investment dollars of venture capitalists, startups, and enterprises who all agree: Something interesting will happen, and with diligence and groundwork planning, we can be ready to act when the future finally arrives.

Data-sharing made easy

SHARE AND THRIVE

Pooling data with others drives new opportunities.

MONETIZE YOUR DATA ASSETS

Data platforms offer a secure mechanism for buying and selling data.

KEEP DATA SAFE

A growing array of privacy-preserving technologies can help keep shared data safe and secure.

TREND 1

Data-sharing made easy

Powerful data-sharing and privacy-preserving technologies usher in a new era of data monetization

Thanks to advances in data-sharing technologies, you can buy and sell potentially valuable information assets in highly efficient, cloud-based marketplaces. Combine this data with a new array of privacy-preserving technologies, such as fully homomorphic encryption (FHE) and differential privacy, and you can now share encrypted data and perform computations on it without having to decrypt it first. This provides the best of all potential worlds: sharing data while preserving security and privacy.

All of this has fueled a promising new trend. Stores of sensitive data lying fallow in servers around the globe due to privacy or regulatory concerns are starting to generate value across enterprises in the form of new business models and opportunities. During the next 18 to 24 months, we expect to see more organizations explore opportunities to create seamless, secure data-sharing capabilities that can help them monetize their own information assets and accomplish business goals using other people's data.

Though currently in an early stage, this data-sharing trend is picking up steam. In a recent survey, Forrester Research found that more than 70% of global data and analytics decision-makers are expanding their ability to use external data, and another 17% plan to do so within the next 12 months.[1]

Moreover, the global FHE market alone is growing at an annual rate of 7.5% and is expected to reach US$437 million in value by 2028. Currently, the health care and finance sectors are leading most FHE explorations.[2]

More than 70% of global data and analytics decision-makers are expanding their ability to use external data.

What accounts for this growth? Simply put, data gains value when it is shared. Gartner™ predicts that by 2023, organizations that promote data-sharing will outperform their peers in most business metrics.[3]

Consider the following examples of data-sharing in action:

- **Using aggregated data to securely achieve common goals.** Organizations can work with "frenemies" within a market sector to achieve common goals such as developing deeper customer insights or detecting fraud patterns across an entire sector.

- **Increasing efficiency and lowering costs.** Across enterprises, data vendors no longer have to provision hardware, maintain databases, and build application programming interfaces (APIs). Customers can push a button to access anonymized, curated data feeds. Within the enterprise, encrypted data makes artificial intelligence (AI) and machine learning (ML) exercises safer, and compliance audits easier.

- **Broadening your research collaboration.** Sharing basic foundational or early-stage findings can accelerate critical research initiatives without compromising a hard-won competitive advantage.

- **Securing intellectual property.** Super-sensitive data such as AI training data that may be stored in public clouds can be better protected.

- **Encrypting data in motion.** In the arenas of high-frequency trading, robotic surgery, and smart factory manufacturing, confidential data flows rapidly across multiple entities. FHE allows users to access critical data quickly without encryption keys.

Opportunities like these to monetize data through sharing and pooling can offer a competitive advantage for first movers—a motivating concern these days across markets. It is not uncommon for new participants in data-sharing ecosystems to experience what has been described as an "oh, sweet Lord moment" upon realizing that their competitors operating on the same platform are doing much more with data assets. In this moment, many resolve to become the best AI- and data-driven organization possible.

Share and share alike

As the lifeblood of digital transformation, data looms large in Deloitte's *Tech Trends* reports. In *Tech Trends 2021*, for example, we discussed how in order to realize their MLOps ambitions, companies must manage their data very differently.[4] Today, the data-sharing revolution is making it possible for organizations to access

more data, more securely within their own ecosystem and across other organizations. But, once again, reaching this potential requires managing data differently—this time adding innovative technologies and techniques that free information assets from traditional privacy and security restrictions.

This year's data trend comprises three major dimensions: **opportunity**, **ease of use**, and **privacy**.

Share and thrive: The promise of new business models and opportunities

Shared data can create shared opportunities and new business models. As the data-sharing trend advances, we expect more organizations to engage in "data collaboration" to tackle common challenges and pursue mutually beneficial revenue, operational, and research opportunities. Moreover, the ability to share data safely with external data management service providers can help organizations streamline data management processes and lower related costs. Consider the following opportunities data-sharing can drive:

- **Industry vertical marketplaces.** Even the fiercest of competitors often share common challenges that are best resolved through collaboration. Take suppliers in the food industry: If they all anonymized sensitive sales and delivery data and pooled it together for analysis, perhaps they could unlock the mystery of supply and demand. Or banks in developing regions could pool anonymized credit data to build an interbank credit risk scoring system. Or one of the biggest opportunities of all: Could pharmaceutical researchers and doctors operating within a secured ecosystem pool data to understand how to bring life-saving innovations to market more quickly?

As the data-sharing trend advances, we expect more organizations to engage in "data collaboration" to tackle common challenges.

- **Partners in a value chain.** Many manufacturers and retailers purchase consumer data from third-party data brokers, but as is often the case, there is not enough quality data to really make an impact. What if systems of partners within a value chain—from suppliers to manufacturers to marketers—pooled their customer data to create a more nuanced picture of demand?

- **Let somebody else do the AI model training.** AI models are often considered highly sensitive forms of intellectual property. Because they can typically fit on a thumb drive, they also represent high security risks, so many organizations have traditionally performed their own modeling in-house. Thanks to encryption technologies, this may be about to change. With modeling data secured, chief data officers can safely outsource AI modeling and training to third parties.

- **Data providers streamline deliveries.** On data-sharing platforms, buying access to real-time market or logistics data is as simple as pushing a button. Data providers will no longer need to provide APIs or ship files.

Acquire external data easily at the push of a button

Cloud-based data-sharing platforms are helping organizations seamlessly share, buy, and sell data. These heavily virtualized, high-performance data marketplaces are typically structured in a data-sharing-as-a-service model in which, for a fee, service subscribers can manage, curate, and tailor data. They can also secure their data to a degree by using platform-provided "clean rooms," safe spaces with defined guidelines where organizations can pool their data assets for analysis. Finally, subscribers can aggregate and sell access to their data to other subscribers. Data buyers get *à la carte* or custom views into different aspects of markets, products, or research.

The fundamental business strategy underpinning this "sharing-as-a-service" model has already demonstrated its effectiveness in other high-profile information and content-sharing arenas such as music file-sharing and social media. In these, a vendor provides an easy-to-use data-sharing platform, and customers provide the content (data).[5]

The data marketplace sector is currently in an early gold rush phase, with startups such as Databricks, Datarade, Dawex, and Snowflake, and hyperscale cloud providers such as AWS, Azure, Google, and Salesforce racing to stake their claims in this promising market. And promising it is: The nexus of data growth and democratization, along with digital transformation, is helping create a revolution in which demand for external data

is skyrocketing.[6] No longer merely a tool for informing executive decision-making, data is now a business-critical asset to be sold, bought, traded, and shared. And the platform that facilitates this exchange most easily and effectively could eventually become the standard for data-sharing in industry data verticals or even across entire markets.

We're seeing data-sharing use cases—and in some areas, success stories—proliferate as more organizations begin pursuing opportunities to monetize and expand their data assets. For example:

- During the early days of the COVID-19 pandemic, fiercely competitive global pharmaceutical firms explored ways to share pre-clinical research data via data-sharing platforms.[7]
- COVID-19 vaccine administrators used centralized state-operated platforms to share daily micro-level vaccination and testing data with public health care agencies.[8]
- Investment managers at a global financial services firm capture and analyze data from their back, middle, and front offices in real time. As a result, the time required to begin sharing investment data with clients shrinks from "months to minutes."[9]

It remains to be seen how certain aspects of the data-sharing platform market will evolve. While there will eventually be some consolidation and standardization, multiple platform markets could also take root. For example, there could be systems of partners in private data marketplaces, or perhaps public marketplaces targeting unique needs will spring up organically. Whatever shape data marketplaces eventually take, we anticipate that the gold rush will continue to pick up steam, particularly as vendors develop ironclad security and more organizations sign up for these platforms, thus expanding the volume of external data available for consumption.

Share data without compromising privacy

Data gains value when we share it. Yet data privacy policies and competitive secrecy demands have historically placed a damper on our ability to realize this value. Today, a new class of computational approaches collectively known as *privacy-preserving computing* (or confidential computing) is poised to liberate organizations and their data from privacy's shackles. Approaches such as FHE, differential privacy, and functional encryption make it possible for organizations to reap the benefits of data-sharing without sacrificing privacy (figure 1).

Figure 1

Six privacy-preserving techniques for sharing data

Fully homomorphic encryption: Data is encrypted before it is shared. It can be analyzed, but not decoded into the original information.

Differential privacy: Noise is added to the dataset so that it is impossible to reverse-engineer the original inputs.

Functional encryption: Select users have a key that allows them to view some parts of encrypted text.

Federated analysis: Parties share insights from their analysis without sharing the data itself.

Zero-knowledge proofs: Users can prove their knowledge of a value without revealing the value itself.

Secure multiparty computation: Data analysis is spread across multiple parties such that no single party can see the complete set of inputs.

Source: Deloitte research and analysis.

Privacy-preserving techniques can also enable collaboration among competitors. Consider multiple financial institutions that compete head-on in distinct areas of financial services. Even though they compete for clients, collectively they may wish to collaborate to achieve common goals such as detecting overconcentration risk, sophisticated fraud patterns, or financial crimes.

In another example, consider organizations that do not compete but belong to complementary companies within an industry sector such as travel. There are beneficial data-sharing use cases in which companies contribute information to co-marketing and discount campaigns across airlines, hotels, and rental car agencies. Each participating company would like to know about the client behavior and activity of the others so they can provide their end consumer with greater value and a more enjoyable customer experience. Yet each has a duty to

protect client information. Privacy-preserving computing may be the breakthrough catalyst that allows these companies to interact and collaborate more deeply.

Currently, four challenges are slowing progress in the field of privacy-preserving computing:

1. Many of these techniques require new software tools and changes to utilize the data. Being able to fully utilize these tools and support the changes can require significant time and effort from already-busy teams.

2. Privacy-preserving techniques can, in some instances, slow speed and performance, which can be problematic with data-in-motion and real-time analysis and dissemination.

3. There is currently no easy way to maintain control over the governance and usage of data once it is in someone else's hands, which raises potential privacy or compliance risks.

4. Finally, there are certain regulatory roadblocks around privacy and data ownership that will need to be addressed before privacy-preserving compute can reach its full potential.

Yet work is underway on all these fronts, and it is not unreasonable to say that within the next 18 to 24 months, privacy-preserving computing will offer a broad range of use cases and opportunities.

The way forward

Though privacy-sharing computing and advanced data-sharing technologies are already helping organizations positioned at the vanguard of this trend extract more value from data, they are not a panacea for all data management requirements and challenges. You will continue to need strong data governance; tagging and metadata are still necessary.

What's more, the new tools and approaches do not change longstanding company data culture overnight. For example, established companies often have entrenched processes and standards for managing and using data, whereas startups and digital natives may take more relaxed approaches. Or, due to the very personal relationships that inform decision-making and strategy, family-owned businesses are typically more hesitant to share data—however anonymized beyond enterprise walls.

We anticipate that these and similar issues are just bumps on the road to a fundamentally new era of transformative data-sharing. You have an untapped asset sitting in your servers. What are you waiting for?

LESSONS FROM THE FRONT LINES

CVS builds on data foundations to distribute vaccines

With nearly 10,000 stores across the United States and proven success in annually administering flu and other vaccines, CVS Health (CVSH) was well positioned to make a significant contribution to the historic COVID-19 vaccine rollout. Still, when vaccines became widely available in the spring of 2021, the pharmacy and retail giant needed analytics immediately to understand when and where immunizations were needed most. Karthik Kirubakaran, senior director of retail data engineering, says the organization's data management processes and technology met the challenge: "Because we had an effective data strategy in place, we were able to extend our capabilities and roll out a new system in weeks instead of months."[10]

Kirubakaran and his team gathered external data from vaccine suppliers and the Centers for Disease Control and Prevention (CDC) to forecast supply and demand. They then fed this information into internal systems that enabled patients to schedule appointments, partners to set up clinics, and analysts to measure campaign effectiveness. The team also shared data externally with research agencies and universities to help gauge vaccination rates in the population. All of this was done at an unprecedented pace during the pandemic. Fortunately, CVSH's data organization capabilities enabled it to rapidly make sense of incoming data, while data-sharing tools provided secure, near–real time exchange. "We were able to move quickly by creating a data mesh across multiple platforms, instead of consolidating to any single technology," says Kirubakaran.

The team established governance immediately to prioritize data protection and compliance with privacy and data security laws. It also identified clear owners and stewards and created different layers of security for data in transit and at rest. For example, it leveraged third-party clean-room technologies to anonymize data for analysts, who then measured the rollout program based on demographic segments instead of individual identities.

CVSH faced new challenges as the vaccine rollout continued. Before each successive distribution of doses to retail stores, Kirubakaran's team huddled in a virtual war room to pore over

demographic and demand data to identify underserved areas. "It was critical for us to create forecasts that were as accurate as possible and facilitated access to vaccines where they were needed," says Kirubakaran. His team then updated its predictions based on supply information from each store, and even analyzed internet searches for COVID-19 vaccine availability to know where demand was high.

CVSH plans to leverage its data-sharing know-how for other use cases as the vaccine rollout slows down. For instance, Kirubakaran's team is working to use real-time data to understand a customer's basket in the retail store and match it to past purchase behavior for more accurate coupons at checkout. He's guided by a CVSH leadership directive asking all CVSH employees to treat customers as someone they can serve instead of someone they can sell to. Says Kirubakaran, "The idea is to serve the community, to do it in a way that is seamless to the customer, and only tap into the data that they allow us to access."

Catena-X changes the automotive value chain collaboration model

European automakers are members of a mature industry; their manufacturing practices are fine-tuned, meticulously planned, and just-in-time, which doesn't leave much room for the unpredictability of the past year. Facing the dual crises of COVID-19 supply delays and semiconductor shortages, the European automotive industry needed to react quickly, but information across the entire automotive value chain, from suppliers to customers to recyclers, was sparse. Several key manufacturers, suppliers, and tech companies, including BMW and Siemens, joined forces to devise a new way of working. Twenty-eight partners launched "Catena-X," a data exchange ecosystem that enables organizations to share information on their own terms, with privacy and security guaranteed. "We needed a collaboration platform to work with value chain partners, one that opened up a new playing field," says Oliver Ganser, head of the Catena-X consortium.[11]

Catena-X, which is Latin for "chain," launched in August 2021 as one of the first major use cases of the European Union's federated and secure data-sharing standard, known as GAIA-X.[12] This decentralized approach comprises a multitude of individual platforms, all following a common EU standard. Organizations using GAIA-X can exchange data and collaborate across sectors while retaining data sovereignty. "Instead of companies developing trust in each other individually, we can all trust our data to the GAIA-X framework," says Ganser.

While GAIA-X provided the standards needed, small and large players ultimately decided to join Catena-X to address their supply chain issues. In one instance, an auto manufacturer found a quality issue that potentially affected tens of thousands of its vehicles. It would normally conduct a major recall and levy millions in penalties to suppliers, but by collaborating with suppliers to share data, the manufacturer was able to pinpoint the quality issue and reduce the number of vehicles that needed a recall by more than 80%.[13]

In the near future, Catena-X will provide a user-friendly system environment that can integrate with enterprise resource planning to transfer data, as well as a software-as-a-service–like portal where smaller suppliers can directly upload data. As new companies join and partners are connected from different areas of the value chain, the consortium anticipates creating new business models. For example, partners may pay incentive fees for sharing data with certain parameters, and sustainability and circular economy is another major use case. "The biggest reason for organizations to join is to solve complex business problems with shared data. Monetizing the data is not our priority," says Ganser.

The Catena-X board is cognizant that change can be hard for a storied industry like German manufacturing. "This is not just technology; this is a transformation of the automotive industry," says Claus Cremers, a Catena-X board member and director at Siemens.[14] The board is dedicated to rethinking the value chain and encouraging its members to adopt a startup mentality. Eventually, its goal is to expand out of Europe into global collaboration and acceptance. "We will always produce cars, but we can re-invent ways to run our overall business instead of relying on past methods," says Ganser.

DARPA revs up data encryption

The Defense Advanced Research Projects Agency (DARPA) has a history of shaping emerging technologies. The agency—which is part of the US Department of Defense—sponsored research that helped create everything from the internet and the personal computer to drones, GPS, and much more. Currently, DARPA is responding to the expansion of cloud computing and other virtual networks by researching new methods for sharing data while lowering privacy and security risk. Dr. Tom Rondeau, program manager at DARPA, believes building trust through privacy-preserving techniques is key to democratic values. "Being able to share information in a way that preserves privacy and security is foundational to democracy," says Rondeau.[15]

Rondeau leads the Data Protection in Virtual Environments (DPRIVE) program, which funds startups and incumbents to create hardware that can enable advanced encryption techniques. Standard encryption techniques keep data safe in transit or in storage, but require users to decrypt data for computational use, which exposes it to cyberthreats. In contrast, DPRIVE is focused on enabling fully homomorphic encryption (FHE), a technique that keeps data protected even during computation. Until now, it could take months of computation time to apply the FHE technique to sensitive data stores. DARPA aims to cut down that time drastically by creating specialized chips and coprocessors. Once this privacy-preserving tech is available and it's embedded into phones and tablets, data can be captured and stored securely on every consumer device, with only encrypted data sent elsewhere for analysis. "If we can accelerate FHE execution, the technique can become a fundamental part of our data-processing approach to almost every application," says Rondeau.

With FHE, the DPRIVE team is creating standards of security by rigor, meaning computational difficulty, so users know just how secure their data is. Understanding levels of security should be like buying a safe, according to Rondeau. Safes are rated by how long it takes for a skilled burglar to break through. Their security rating helps buyers make better decisions around safeguarding valuables. Similarly, if data management teams know how long it takes to hack into different kinds of encryption, they can determine which information requires the most security, and how often encryption codes should be changed to prevent hacking. "We should be able to prove exactly how secure something is, not just for consumers to feel protected when using their devices, but also for better measuring our national security," says Rondeau.

DPRIVE offers a key use case for securely sharing data on national security threats with other governments. "FHE could become a way of sharing intelligence data from the field while protecting our sources and techniques for gathering intelligence," says Rondeau. Similarly, in the case of financial crime analysis, law enforcement agencies need data to analyze crimes, while banks are mandated to protect their consumer data. Rondeau believes advanced encryption techniques could make it possible for both parties to share and analyze the data needed to identify money laundering without compromising privacy.

Today, FHE computation is very computationally intensive and too slow for many use cases. Though DARPA is working with partners to solve this technical problem through better hardware, scaling up the solution is the organization's end goal. Rondeau and his team believe that once privacy-preserving tech, techniques, and standards are commonplace, they can improve everyone's privacy over time. Says Rondeau, "This is a technology that can support and export our democratic principles on the security and privacy of information. It can do a lot of good."

MY TAKE

Kyle Rourke

Vice president of global platform strategy, Snowflake

As the vast majority of enterprise computing moves to hyperscalers, the world's data is consolidating via cloud providers into a handful of physical data centers.

This transition alone, though, doesn't make the data any easier to access and unlock for monetization across organizations. At Snowflake, we recognized a decade ago that to share and utilize data effectively, organizations need to be part of a network with built-in trust and governance, underpinned by a technology that eliminates data silos.

Snowflake has always enabled organizations to store and analyze their data in the cloud. As customers realized massive performance and concurrency gains, their appetite to leverage even more data, including data owned by other organizations, has increased. Last year, we unveiled our foundational technology that creates a single network which every customer can connect to, akin to one massive relational database, or a sort of social network for data. This made it possible

for organizations to share data with others in real time, if they choose, by simply granting access within the platform. We've watched the number of interorganizational connections grow rapidly.

By sharing or combining data with others, organizations are now developing a variety of innovative products and services. For example, a company that gathers location analytics can distribute data at the click of a button to rideshare companies that want to know where drivers are most needed. Media publishers can combine their customer data with data from retailers to create a new dataset that allows both organizations to better target their ads and products. Going forward, data networks can grow like social networks: Exponential adoption will drive value creation in new and unexpected ways.

Across the industry, the methods of sharing data are evolving. In the past, organizations would have to find secure ways to gather data, copy and upload it to their own servers, ensure their data collection was compliant with policies, and more. As marketplaces for live data continue to grow, organizations can buy or sell data as a service without the costs of ingestion, maintenance, and compliance. With less friction in the way, organizations are free to become more creative. Data that was traditionally siloed within just one company will now be unlocked for the benefit of the many, and we're yet to see *what* novel, lucrative uses will result.

Of course, organizations cannot share most data without privacy measures in place. Data networks like ours require strong governance to facilitate trust and willingness to share. Clean rooms bring data together from multiple companies for joint analysis under guidelines that keep the data secure. Restricted queries can prevent drill-down into sensitive data such as PII while allowing analysts to gather anonymized records to feed into their models.

Eventually, the ability to run analyses or create models using data from outside the enterprise will become commonplace. Our customers are increasingly telling us where to go next as they explore different ways of collaborating on data. The change we're seeing now is similar to how the internet unlocked and democratized access to information: The ability to collaborate and operate in a safe, compliant, trusted way with data is going to open up radical new possibilities for business.

EXECUTIVE PERSPECTIVES

STRATEGY

CEOs should keep a lookout for new business models emerging from data-sharing. If today's data exchange platforms become the next generation of barcodes, opportunities may arise to monetize data or open new partnerships. It will be important to determine whether to be an early entrant or a fast follower of the new data paradigm. Depending on what makes sense for their business, participating in this trend early on can dictate the terms of how data-sharing is accomplished.

FINANCE

Some CFOs may view the trend toward data-sharing with trepidation, worrying about threats to market competitiveness, regulatory compliance, and company reputation. However, as new data-sharing business models proliferate, CFOs will want to work with their technology and risk counterparts to identify the right opportunities for sharing. As this trend expands, CFOs should weigh the long-term benefits and risks of sharing data, which could significantly impact organizational growth and even survival.

RISK

In the past year, high-profile cyberattacks have shut down entire supply chains. Third-party risk management will be more crucial than ever as supply networks and attack surfaces expand. Chief risk officers (CROs) should work with IT teams to promote sharing data, security vulnerabilities, and standards across their vendor networks. By driving greater visibility and awareness, CROs can better prepare organizations to respond to future supply chain risks while applying the latest privacy-preserving and security technologies.

ARE YOU READY?

KEY QUESTIONS

1 Which data assets could you share with partners to tackle common challenges and pursue mutually beneficial revenue, operational, and research opportunities?

2 Have you leveraged external data from data marketplace platforms to augment your own data assets? How did access to more information enhance your decision-making process?

3 Which privacy-preserving computing techniques are you using? How has or would the ability to analyze anonymized data enable new use cases and innovative experimentation?

LEARN MORE

Data as a strategic asset
Learn how organizations who approach data as a strategic asset drive new efficiencies, insights, and capabilities.

Machine data revolution
Explore how tuning data for native machine consumption helps to achieve the benefits and scale of AI and MLOps.

MLOps: Industrialized AI
Gain insights into applying an engineering discipline to automate machine learning model development, maintenance, and delivery.

AUTHORS

Our insights can help you take advantage of emerging trends. If you're looking for fresh ideas to address your challenges, let's talk.

Frank Farrall
AI ecosystems leader
Deloitte Consulting LLP
frfarrall@deloitte.com

Juan Tello
Chief data officer
Deloitte Consulting LLP
jtello@deloitte.com

Nitin Mittal
US AI strategic growth offering leader
Deloitte Consulting LLP
nmittal@deloitte.com

Eli Dow
Analytics and cognitive technology fellow
Deloitte Consulting LLP
elimdow@deloitte.com

Chandra Narra
Managing director
Deloitte Consulting LLP
cnarra@deloitte.com

SENIOR CONTRIBUTORS

Tiago Durão
Partner,
Deloitte & Associados, SROC S.A.

Marcin Knieć
Director,
Deloitte Poland

Rajeev Pai
Director,
Deloitte MCS Limited

Markus Schmidthuysen
Director,
Deloitte Consulting GmbH

Vivek Shrivastava
Partner,
Deloitte India

Rajeev Singhal
Partner,
Deloitte & Touche LLP

Yves Toninato
Senior director,
Deloitte Belgium CVBA

Jeroen Vergauwe
Partner,
Deloitte Belgium CVBA

Dinesh Dhoot
Specialist leader,
Deloitte Consulting LLP

Lakshmi Subramanian
Senior manager,
Deloitte Consulting LLP

Karl-Eduard Berger
Manager,
Deloitte France

ENDNOTES

1. Jennifer Belissent, *Chief Data Officers: Invest in your data sharing programs now*, Forrester, March 11, 2021.
2. Data Bridge Market Research, *Global fully homomorphic encryption market – Industry trends and forecast to 2028*, March 2021.
3. Laurence Goasduff, "Data sharing is a business necessity to accelerate digital business," Gartner, May 20, 2021. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.
4. Christina Brodzik, Kristi Lamar, and Anjali Shaikh, *Tech Trends 2021: Disrupting AI data management*, Deloitte Insights, December 2021.
5. Michael Gorman, "Data marketplaces will open new horizons for your company," *VentureBeat*, December 23, 2020.
6. Tomas Montvilas, "Understanding the external data revolution," *Forbes*, June 25, 2021.
7. Dr. Nicola Davies, "Covid-19: The importance of data sharing within the pharma industry," Data Saves Lives, June 26, 2020.
8. California Immunization Registry, "Covid-19 vaccine reporting information and resources," California Department of Public Health, accessed November 5, 2021.
9. Snowflake, "State street accelerates investment insights by building alpha data platform," accessed November 5, 2021.
10. Karthik Kirubakaran (senior director of retail data engineering at CVS Health), phone interview, September 22, 2021.
11. Oliver Ganser (head of the consortium, Catena-X) and Claus Cremers (board member of Catena-X) interview, September 15, 2021.
12. Gaia-X, "What is Gaia-X?" accessed November 18, 2021.
13. Ganser and Cremers interview.
14. Ibid.
15. Dr. Tom Rondeau (program manager at DARPA), phone interview, October 26, 2021.

Cloud goes vertical

CLIMB THE STACK

Cloud vendors are automating and abstracting ever-higher order business processes to create industry-optimized platforms.

DOUBLE DOWN ON DIFFERENTIATION

By cloud-sourcing commodity industry processes, CIOs can refocus talent and budget on the systems that create competitive advantage.

BUILD THE CAPACITY TO CHANGE

Cloud-based capabilities can help organizations create the capacity to think bigger by acting smaller. Less custom code means more agility.

TREND 2

Cloud goes vertical

Industry-specific cloud solutions can enable organizations to automate manual tasks and shift their focus to competitive differentiation

As the global economy moves from a pandemic footing to a more future-focused endemic one, many organizations are looking for opportunities to become more nimble and efficient by offloading business processes to the cloud.[1]

In response, cloud giants, software vendors, and system integrators are developing an array of cloud-based solutions, accelerators, and APIs that are preconfigured to support common use cases within industry verticals.[2] These solutions are designed specifically for easy adoption, and can be built upon to create digital differentiation.

Whatever mix of *à la carte* applications, tools, or services users adopt from these offerings, cloud becomes the fabric stitching them together into powerful business process solutions. For example, a global automobile manufacturer has partnered with cloud vendors to develop cloud-based connected car application development services for the transportation industry. The platform features industry-specific solutions along with IoT, machine learning, analytics, and compute services that manufacturers can leverage to develop connectivity layers for their vehicles.[3]

The health care industry initially deployed cloud processes for managing back-office data. Regulatory compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) drove the next phase of this sector's cloud journey as health care organizations began managing patient data in the cloud. Today, pioneering health care providers are exploring ways to use cloud-based HIPAA models to improve medical treatments.[4]

Over the next 18 to 24 months, we expect to see a growing number of organizations across market sectors begin exploring ways that industry clouds can help them meet unique vertical needs. Indeed, based on Deloitte analysis, we project that the value

of the industry cloud market could reach US$640 billion within the next five years.[5]

Clearly, the *Cloud goes vertical* trend is gaining momentum, so the time to begin exploring its possibilities for your organization is now. You can start by performing an assessment of your business process ecosystem to determine which processes you would consider cloud-sourcing from external vendors, and the pros and cons of doing so.

As a critical part of this assessment, try to gauge how well current processes support your short- and long-term business strategies, and where there is room for improvement. Moreover, keep in mind that the rapidly growing menu of cloud-based capabilities could spark new business models and out-of-the-box possibilities.

Finally, the industry cloud trend presents a long-overdue opportunity to restructure IT. As companies begin outsourcing IT functions and business processes that provide no competitive advantage, they can redirect their efforts and investments to "differentiating" systems and services that do, while simultaneously creating a lasting capacity to change.

This assessment doesn't need to be some monolithic, two-year project. Indeed, it can be done in bite-sized increments that add efficiency and effectiveness to most processes along the way. At the same time, you can begin refocusing talent and resources toward the differentiated processes that deliver competitive advantage.

From infrastructure to industry verticals

The business and technology needs currently driving the *Cloud goes vertical* trend are not new. Starting in the 2000s, organizations with similar compliance, business process, or data management needs began adopting cloud-based software. At roughly the same time, CIOs began "lifting and shifting" some on-premises systems to public clouds in order to lower costs and gain efficiencies.

Today, the twin approaches of sharing software that meets common needs and letting someone else run your infrastructure continue to inform the *Cloud goes vertical* trend. What's new is that we've moved from procuring generic functions and libraries to the digitization and availability of actual industry-specific business processes. Moreover, organizations increasingly expect cloud vendors to create "common core" solutions that address shared needs across industries and ecosystems. Hence, cloud and software vendors now offer an expansive menu of industry-specific, modular business processes available through APIs that can be accessed at the push of a button. For example,

using APIs, engineers and system architects can connect targeted smart factory systems together in a shared cloud network. Surgical capabilities like these represent a quantum leap from FedRAMP-esque, compliance-based offerings just a few years ago.

Against this background, we see this trend unfolding in the following dimensions:

Hyperscalers climb the stack

The "big three" cloud services providers—Amazon Web Services (AWS), Google Cloud Platform, and Microsoft Azure—offer cloud-based industry enclaves that automate business processes that are unique to sectors like health care, manufacturing, automotive, retail, and media, among others.

They began by creating infrastructure-as-a-service (IaaS) capabilities, which eventually elevated to platforms-as-a-service (PaaS). But they haven't stopped there. Hyperscalers have continued to climb the technology stack, methodically automating ever-higher order processes to create industry-optimized platforms that are, in some cases, more functionally robust and efficient than the on-premises solutions businesses are currently running. For example, some in the hospitality industry now utilize cloud-based reservations and customer management systems. Likewise, the manufacturing sector takes advantage of cloud-sourced predictive maintenance solutions.

Organizations will find much more than hyperscaler-developed products and services in industry clouds. Indeed, there is a growing ecosystem of sector-specific business capabilities from established vendors such as MuleSoft, Oracle, Salesforce, SAP, ServiceNow as well as startup and open-source projects.[6]

Focus on differentiation

Chances are you have some home-grown code that you should hang on to. You have invested time and budget developing these capabilities that—thanks to your good planning and execution—deliver competitive advantage. Think of them as keys for differentiating your organization in the market. Say you are a retailer and you've spent considerable time customizing your in-store inventory management engine. The C-suite (and the market) recognize your inventory capability as a best-in-class superpower. Just because your cloud vendor might offer an inventory API doesn't mean you should automatically use it. You own the customized code and it contributes heavily to competitive differentiation. Why not keep it? You can certainly run it in the cloud, but the important thing is that it's your IP, and it meets your unique needs in ways that off-the-shelf offerings cannot.

It's important to assess your options before you act. The spectrum of vertical-focused solutions available today is more sophisticated and granular than it was even a couple of years ago. Think about your existing ability to execute a process. If your current capability is better than what's available off the shelf, then keep your own logic. But if you are competing against digital natives and your process—and the capabilities that support it— are no longer that special, consider using an industry API.

For many technology and business leaders, participating in the *Cloud goes vertical* trend will require a reckoning of sorts. Together, leaders must determine where the company wins in the marketplace, and which technologies make those wins possible. If, for example, you win through nontraditional customer service, then invest heavily in those in-house analytic capabilities; these capabilities deliver competitive differentiation and enable new innovation and revenue generating opportunities. Guard them jealously. By contrast, everything that doesn't separate you in the market becomes commodities and can be provisioned as business services from cloud or software providers.

As you explore the opportunities that the *Cloud goes vertical* trend may offer, consider taking the following steps, some of which may be long overdue:

1. Business and IT leaders should work together to determine where the company wins today and in the future. For this effort to succeed, the business must understand technology more deeply. Likewise, IT must understand business strategy and the critical role that technology plays in advancing it. Only then can both teams identify the technologies that are critical to achieving wins.

2. Create an inventory of business processes and the cloud-based offerings that support them.

3. Identify which differentiating processes and enabling technologies to keep in-house. Likewise, identify areas in your business that could benefit from the emerging suite of technology offerings enabled by the cloud.

4. Work with cloud service providers, software vendors, and integrators to plan the next phase of your cloud journey.

Modern engineering

Even as "buy" evolves into "assemble," there is a need for a different kind of "build." We're not talking about armies of developers working on multiyear projects to build behemoth custom systems. Rather, think of modern software engineering with small teams working with cloud services, platforms, and tools to integrate and deploy quickly.

A big part of this new equation is full stack teams working closely together on a set of well-defined outcomes. Leading organizations embrace "pods" or "two pizza-box teams" in which cloud engineers, UX designers, data scientists, quality assurance, and product managers blur the lines between disciplines as they work together. Team members grow and learn as they lean in on whatever the current sprint requires. Importantly, the teams are collectively focused on solving business problems and shaping the road map of whatever they are working on. This represents a welcome change from simply cranking through solution requirements removed from the "why" and the "so what".

The other key is empowerment. Modern engineers expect autonomy, from a purpose lens (having the choice to work on something they believe in); to a tools lens (choosing what gear, platforms, open source libraries they use to practice their craft); to a personal lens (dress code, hours, remote work arrangement).

When technology leaders from traditional organizations visit high-tech startups, they often take away the wrong lesson. The reason engineering teams at digital native companies often thrive is not because of foosball tables, stocked fridges, or silly perks. It's because these young companies appreciate engineering as a core creative discipline. Moreover, they respect engineers and give them the authority they need to succeed. Of course guardrails and guidelines are still necessary, especially in areas of security, compliance, and legal IP protection. But they are deployed within the larger context of elevating modern engineering as a key part of the organization's strategy and future culture.

Build the capacity for change

In a time of disruption and rapid-fire innovation, access to best-in-class solutions or even experimental tools gives organizations the software options they need to connect all the dots in their multifaceted digital transformation strategies. This access hinges, however, on a capacity to change.

Consider this: Clouds tailored to the needs of specific industry verticals will evolve continuously as innovative solutions and services emerge. To maintain their competitive differentiation, organizations will need to embrace disruption, and stay on top of the latest industry cloud offerings. In a climate of rapid-fire change, the future is always approaching fast. Cloud technology can help organizations create not only the capacity to change, but the agility to do so continuously. The fewer systems and processes you have in-house today, the fewer you will have to manage, upgrade, and refresh tomorrow. Most companies are already in the cloud to some degree. If you are, think of the industry cloud trend as the next leg of your cloud journey, one that riffs on the cloud's original promise of sharing resources to solve problems affordably and at scale.

The way forward

The good news is that fully embracing the *Cloud goes vertical* trend doesn't require some big bang effort. Indeed, it can be done in small, thoughtful steps that help you side-step complicated legacy app renewals or disruptive core modernization initiatives. And with each step, your systems become more efficient and effective.

MY TAKE

Marijan Nedic

Vice president, head of IT business solutions, SAP

I believe what separates you from your competitors is not the majority of your operations; it's the 5-to-10% of your operations that are unique.

The emergence of industry clouds—packaged solutions of common applications and configurations used across a given vertical—is helping businesses spend less time setting up the table-stakes functionality necessary for running their businesses and more time on the impactful areas that set them apart. At SAP, our goal is to create industry clouds that enable our clients to meet most needs out of the box, plug easily into partner solutions, and manage unique differentiators in a consolidated platform.

Whether you run a hospital, factory, car rental company, or any other type of enterprise, odds are many of your processes and operations are nearly identical to those of your competitors.

Therefore, the industry predefines most of your problem space. And most of that problem space has already been solved.

As such, any industry cloud worth its salt will have a few common features. First, the industry cloud must provide most of the functionality needed for the industry out of the box, especially the commodity functions. Second, it must be an open platform that enables customers and partners to develop innovative solutions. The platform needs to make it easy to connect and manage these solutions. Third, it should allow customers to ramp up or scale down capacity and processes according to demand. Finally, it should enable easy access to other business and technology services. For example, all the major cloud services today include common tools straight out of the box. While natural language processing (NLP) is now a common tool, the question is how to integrate NLP into your business. Across all these features, your industry cloud should support your broader ecosystem.

I recently visited a manufacturing client that utilizes agile production methods to respond to both large and small customer orders. It's a very profitable business but it requires frequent reconfiguration of production lines. To optimize equipment performance, machine learning (ML) models analyze order data to determine necessary machine configurations and the optimal sequence for filling orders. The process works exquisitely, but it took a massive effort from the manufacturer's digital team to build it all by hand.

Instead, these capabilities can be derived from a single industry cloud. Offloading much of the building and maintenance of these processes can give data scientists more time to develop ML models that help the factory respond more quickly to orders. If machine vision is combined with ML models, quality control teams can inspect a greater percentage of goods coming off the line. Spending more time on activities that really matter helps manufacturers scale their operations more rapidly than if they build functionality manually. These are the kinds of things that set a manufacturer apart.

With this combination of functionality in place, businesses can become more agile. When their main operational platform comes configured for the needs of a typical business in their industry, they can focus their energies on the portion of their operations that sets them apart. They can get straight to a digital representation of their business, their network of partners, their network of suppliers, their machines. Ultimately, it's about having the agility to develop the innovations that can truly make your organization unique.

EXECUTIVE PERSPECTIVES

STRATEGY

Cloud and software vendors are developing increasingly sophisticated and capable business functions as a service. With new opportunities for more sophisticated outsourcing, CEOs must clarify their organization's unique value proposition. Just as ERP standardized most back-office functions, leaders must identify which subset of their business functions are differentiators. Only now, the stakes are higher: the divisions being replaced are not finance or accounting, but those that comprise the heart of the business and influence strategic decisions.

FINANCE

CFOs interested in budget and compliance requirements may find two-fold benefits in cloud-based applications customized to industry needs. Industry clouds can help companies keep pace with technology and regulatory changes with less effort, freeing up talent for more value-added projects. CFOs should ensure close collaboration between finance, IT and compliance, risk, and legal functions so that all parties understand how to maximize the potential benefits of new cloud services.

RISK

CROs have an opportunity to integrate cyber risk management at the onset of new industry cloud deployments. Vendors' standard cybersecurity components may not meet an organization's application needs. As industry clouds drive more business functions, tailored cloud security is becoming more important. CROs and IT can make cybersecurity a differentiator of the organization's cloud tech stack instead of an afterthought. Especially for consumer-facing organizations, building in cyber protection at the onset can prove less costly in the long run.

ARE YOU READY?

KEY QUESTIONS

1 What nondifferentiating processes do you currently support that others in your industry also support? Do the vendors with which you have relationships offer industry-tailored solutions that could be more cost-effective?

2 What technologies are critical to your ability to win in the coming years? How can you redirect more financial and development resources to these areas? Should you keep them in-house, or move them to the cloud?

3 Are you ready for a future that is always "fast approaching"? What changes can you make to your digital transformation strategy to create and nurture the capacity for change across systems and processes?

LEARN MORE

Reimagining digital transformation with industry clouds

Learn how leveraging industry clouds can maximize your transformation strategy by focusing on what you do best.

Awakening architecture with cloud innovation core

See how organizations can reach their technology innovation targets by considering the latest in leading cloud native approaches.

Deloitte on Cloud blog

Reimagine what cloud can do for your business with real-world insights and expert opinions.

AUTHORS

Our insights can help you take advantage of emerging trends. If you're looking for fresh ideas to address your challenges, let's talk.

Ranjit Bawa
US cloud leader
Deloitte Consulting LLP
rbawa@deloitte.com

Mike Kavis
Chief cloud architect
Deloitte Consulting LLP
mkavis@deloitte.com

Brian Campbell
Strategy principal
Deloitte Consulting LLP
briacampbell@deloitte.com

Nicholas Merizzi
Cloud strategy principal
Deloitte Consulting LLP
nmerizzi@deloitte.com

SENIOR CONTRIBUTORS

Steve Rayment
Partner,
Deloitte Australia

Benjamin Cler
Senior manager,
Deloitte Luxembourg

Jorge Ervilha
Manager,
Deloitte & Associados SROC, S.A.

Senthilkumar Paulchamy
Manager
Deloitte Consulting LLP

ENDNOTES

1. According to the Flexera 2021 report *Cloud computing trends: 2021 state of the cloud report*, 90% of enterprises expect cloud usage to exceed prior plans due to COVID-19.
2. Kash Shaikh, "Industry clouds could be the next big thing," *VentureBeat*, March 28, 2021.
3. Ford Motor Company, Autonomic, and Amazon Web Services, "Ford Motor Company, Autonomic, and Amazon Web Services collaborate to advance vehicle connectivity and mobility experiences," April 23, 2019.
4. *Analytics Insight*, "HIPAA compliance, big data and the cloud—a guide for health care providers," September 15, 2021.
5. Brian Campbell, Nicholas Merizzi, Bob Hersch, Sean Wright, Diana Kearns-Matatlos, *Reimagining digital transformation with industry clouds: Organizations can leverage industry clouds to enable strategic transformation and stay on the cutting edge*, Deloitte Insights, November 23, 2021.
6. Bill Briggs, Stefan Kircher, and Mike Bechtel, *Open for business: How open source software is turbocharging digital transformation*, Deloitte Insights, September 17, 2019.

Blockchain: Ready for business

BLOCKCHAIN AT SCALE

Maturing technologies, standards, and delivery models are driving enterprise adoption.

USE CASES BEYOND WALL STREET

As businesses experiment with blockchain, creative use cases are cropping up in multiple industries.

LEAD WITH NEED

Incumbents and startups alike must lead with genuine needs to realize business benefits with blockchain.

TREND 3

Blockchain: Ready for business

Distributed ledger technologies are changing the nature of doing business and helping companies reimagine how they manage tangible and digital assets

Trendy cryptocurrencies and nonfungible tokens (NFTs) capture media headlines and the public imagination, but these and other blockchain and distributed ledger technologies (DLTs) are also making waves in the enterprise. Much like the TCP/IP protocols that provide underlying support to enterprise network communications, shared ledgers could eventually become an integral, if invisible, foundation of business operations, allowing established industry leaders to expand their portfolios and create new value streams and enabling startups to dream up exciting new business models.

Blockchain and DLT platforms have crossed the disillusionment trough of the hype cycle and are well on their way to driving real productivity. They are fundamentally changing the nature of doing business across organizational boundaries and helping companies reimagine how they make and manage identity, data, brand, provenance, professional certifications, copyrights, and other tangible and digital assets. In fact, while companies canceled purely speculative blockchain projects during the pandemic, they doubled down on those delivering proven benefits.[1]

When *Tech Trends* last discussed blockchain, we explored the need for standardized technology, processes, and skill sets to clear the path for adoption and commercialization.[2] Today, technical advancements and regulatory standards, especially in nonpublic networks and platforms, are helping drive adoption by organizations beyond financial services. Maturing technology and platforms are helping advance progress by supporting interoperability, scalability, and security. As enterprises get comfortable with blockchain and DLT platforms, creative use cases are cropping up in many industries, fundamentally transforming the nature of doing business across organizational boundaries.

Blockchain at scale: Evolving technologies and standards

First-generation blockchain and DLTs have proven the feasibility of such applications as cryptocurrency trading, clearing, and settlement—but they have also proven to be slow, energy-hungry, and impractical to scale.

At first, the market teemed with numerous platforms and protocols. However, it lacked technical or process standards and, without interoperability, enterprises could not interact across multiple platforms. Early use cases were constrained to the simple transfer of value from one party to another. Users couldn't create conditional transactions or contingencies that would allow parties to agree on terms.

In addition, adoption was limited by unique challenges associated with transaction verification. For example, cryptocurrencies and other use cases verified transactions using the proof-of-work consensus mechanism, a complex and lengthy computational process that consumes high amounts of energy and has high per-transaction fees and slow transaction times—10 minutes or more for each transaction.[3]

Such challenges are typical of the early stages of adoption of most technologies, and entrepreneurs, enterprises, and academic institutions set out to industrialize blockchain and other DLT platforms. Today, maturing technologies, evolving standards, and new delivery models are boosting enterprise adoption. For example:

Nonpublic and permissioned networks. Many early DLT platforms are low-trust public networks in which anyone can participate. As a result, these networks often include fraudulent members and lack complete privacy and anonymity. Today, risk-averse enterprises have more trusted, secure options: nonpublic (i.e., private) networks, which only allow select, verified members to participate; and permissioned networks, which anyone with a verified identity can join, with member activities controlled via permission-based roles.

Technology improvements. A growing emphasis on usability and speed permits practical use cases not supported by first-generation applications, including the ability to set up self-executing contracts and contingencies. New types of cryptographic processes for verifying transactions consume far less energy than the proof-of-work process and have eliminated bottlenecks, enabling speedier transactions and lower per-transaction fees and energy consumption. For example, the proof-of-authority consensus mechanism is used to verify transactions in many of the private and permissioned networks favored by enterprises.

Improved interoperability. Many DLT platforms suitable for enterprise use have emerged. Polkadot, Cosmos, Wanchain, and many other new protocols and platforms enable enterprises to connect multiple blockchains and seamlessly interact, collaborate, share, and make transactions with multiple entities across numerous platforms. This allows organizations to develop foundational infrastructures that support multiple use cases and customized applications. Architecture, consensus mechanism, token type, and other characteristics vary among platforms, and organizations may need to explore more than one, depending on objectives and use case.

Technology and innovation ecosystems. With the increase in the number of DLT platforms, innovation has grown in tandem, and an extensive, vibrant ecosystem has emerged. Its participants are developing decentralized apps that provide such specialized functions as identity management and supply chain management.

Today, maturing technologies, evolving standards, and new delivery models are boosting enterprise adoption.

Blockchain beyond Wall Street

Enticed by the promise of safer, more efficient transactions, the financial services industry has been leading the way in leveraging blockchain and other DLT platforms.[4] But the benefits extend far beyond Wall Street, especially in uses cases in which multiple organizations access and share the same data and need visibility into transaction history. Typically, this is an expensive, inefficient process lacking trust and security. As the potential emerges for blockchain and other DLTs to bolster the efficiency of business operations and create new ways of delivering value, many forward-thinking companies in other industries are implementing and integrating these technologies into existing infrastructures and road maps.

In fact, the vast majority of participants in Deloitte's 2021 Global Blockchain Survey (80%) say their industries will see new revenue streams from blockchain, digital assets, and/or cryptocurrency solutions.[5] And global spending is soaring, with one research firm predicting that it should increase from US$5.3 billion in 2021 to US$34 billion in 2026.[6] According to another analysis, banking leads in blockchain adoption, followed by telecommunications, media, and entertainment; manufacturing; health care and life sciences; retail and consumer goods; and government. Retail and consumer goods

are projected to see the fastest growth in blockchain spending between now and 2024.[7]

Use cases gaining traction include:

Self-sovereign data and digital personal identity. Leveraging blockchain and other DLT platforms for secure storage and management, users can establish ownership over their personal data and create and control their own tamper-proof digital identities. This can enhance the security of personally identifiable information and prevent the creation of counterfeit or stolen identities. Applications include contact-tracing, electronic health records and credentials, and electronic voting.

Trusted data-sharing among third parties. As discussed in *Data-sharing made easy*, data access and sharing among third parties are typically restricted due to technology silos and privacy concerns. Private and permissioned DLT platforms enable organizations to securely interact with and exchange data, ensuring that verified, trusted third parties have only the specific levels of data access needed. Without sacrificing data integrity or privacy, organizations can share data across company and industry boundaries and enhance collaboration and trust among ecosystem partners. For instance, secure data-sharing among health care providers could improve the exchange of patient health information; in the intelligence community, it could facilitate the exchange of threat intel and other actionable information across agency and international boundaries.

Grant funding. For both funding agencies and grantees, blockchain and other DLT platforms can help reduce the administrative burden associated with monitoring and reporting financial and performance results. One study of federal agency initiatives found that using blockchain to make, track, and monitor grant payments enhanced the quality and transparency of grant reporting and improved the efficiency of payments and reporting.[8]

Intercompany accounting. Intercompany clearance and settlement—especially for large global organizations or those with numerous legal entities—often involve multiple enterprise resource planning systems, spreadsheets, and manual processes; reconciliation frequently is delayed for many weeks after the transaction is complete. Blockchain and other DLT platforms can improve traceability, transparency, and auditability of intercompany transfers accounting, especially in mergers and acquisitions, by validating and creating a shared, immutable record of transfers.

Supply chain transparency. In today's global supply chain, blockchain and other DLT platforms can improve product-tracking and

traceability to reduce counterfeit products and illegal or inferior ingredients and components; ensure the provenance of items such as turkeys, diamonds, and wine; and help governments enforce tariffs and trade policies. It can also help track assets and shipments, allowing for more transparency throughout the procurement process, from purchase orders and logistics to invoicing and payments.

Customer and fan engagement. Selling NFTs as collectibles enables people and organizations to build digital communities, engage fans and customers, and build their brands. When COVID-19 restricted live sports and entertainment events, NFTs helped entertainers and sports personalities, teams, and leagues diversify revenue and stay in touch with their fans and customers.[9] And when used for event ticketing, blockchain and NFTs have the potential to eliminate ticket fraud and scalping.

Creator monetization. Artists, writers, inventors, and other creators often struggle to prove ownership of and monetize intellectual property (IP) through licensing, patents, and copyrights. With blockchain and other DLT platforms, content creators can embed their IP with a smart contract that's executed every time the IP is downloaded. The contract can trigger an automatic payment and flex based on user identity; for example, a large enterprise would pay more than an individual consumer.

Lead with business and customer need

It's possible to draw an analogy between today's DLT platforms and the internet of the mid-1990s—and to the change that the internet brought to business processes across industries and ecosystems.

Consider that in its infancy, the internet was slow, ugly, and misunderstood. Some legacy companies ignored it—after all, they reasoned, there's no market for online shopping or movie streaming. Many startups, on the other hand, enthusiastically joined the party, adding the ".com" suffix to their business names and spending lavishly on business and product launches.

Both of these fairy tales ended badly. However, for every market leader that ignored the internet and fell by the wayside, another savvy incumbent eventually became an online giant. And while internet startups with unsustainable or flawed business models didn't survive the long haul, those with solid business strategies and execution became wildly successful. When the dust of the dot-com era settled, the companies left standing were the ones that built—or rebuilt—their business models around tangible business and customer need.

The current state of blockchain and other DLT platforms is not unlike that of internet in 1997: clunky, with an inadequate user interface, but with lots of possibility for enterprise applications. Like the internet, they're helping businesses and organizations streamline business processes and operations and drive value through the creation of new digital business models. Their ability to build trust outside of organizational boundaries without the use of traditional intermediaries profoundly changes the way value can be created and delivered—and, like the internet, they're transforming how business is conducted across industries and ecosystems. Within a single organization, change can be challenging; across multiple organizations and industries, it likely will be several orders of magnitude more difficult. As barriers to using DLTs fall, both incumbents and new entrants that are *leading with business and customer need* are able to navigate this transformation more smoothly.

Many entrepreneurs and startups are working to identify new customer use cases and develop and gain investors for new business models based on blockchain and other DLTs. For example, startups have created shared ledger–based authorship, and ownership platforms can solve challenges around copyrights, attribution, rights management, and royalty payments that artists, writers, and musicians face.[10] But established market leaders aren't sitting idly while these technologies disrupt their industries. Instead, they're embracing DLT-driven business models and leveraging their reputations as trusted providers. For instance, Microsoft leans on blockchain to provide a record of royalty agreements and payments for its gaming partners.[11]

The way forward

Today, maturing technologies, evolving standards, and new delivery models are boosting enterprise adoption of blockchain and other DLT platforms. A plethora of enterprise use cases continues to emerge, providing organizations across industries the ability to develop new business models that transform value creation of all manner of physical and digital assets and streamline business processes across organizational boundaries. As confidence in the shared ledger grows, could the collective on-chain record one day be viewed as a more credible assertion of truth than an off-chain record?

Innovative business models can help startups break new ground and enable legacy enterprises to evolve or supplement existing business strategies to maintain their reputations as trusted brokers within the "trustless" shared-ledger ecosystem. To be successful, newcomers and old timers alike will likely need to first identify legitimate customer or business needs.

As organizations leverage blockchain and other DLT platforms to drive new business value, they likely will need to understand which platforms and protocols are the most relevant for their industries and use cases, and future-proof existing enterprise architectures to operate in multiple platforms. Finally, to support the cross-organizational and industry transformation that these technologies and platforms will bring, organizations can cultivate a sense of urgency in improving or changing business processes and bolster change management capabilities.

LESSONS FROM THE FRONT LINES

Caisse des Dépôts scales up blockchain programs in French finance

Caisse des Dépôts et Consignations, a public financial institution in France, has established several mature blockchain initiatives. While many companies are still trying to figure out what blockchain is and how it might be useful, the 205-year-old organization is using blockchain to unlock both new opportunities and new ways of operating.

But getting there didn't happen overnight. When Nadia Filali, head of the blockchain and cryptoassets program at Caisse des Dépôts, first heard about Bitcoin and the security protocol that underpins the cryptocurrency in 2015, she recognized the opportunity but knew it would take a team with diverse expertise along with a broad ecosystem of partners. "You can't work on blockchain alone," Filali says. "You have to collaborate."[12]

After talking to several other financial institutions and blockchain startups, Caisse des Dépôts partnered with 10 other organizations to launch LaBChain, a consortium dedicated to exploring opportunities using distributed ledger technologies for the financial services sector. Once all members had a common understanding of the technology through trainings and experiments, LaBChain enabled them to develop proof-of-concept projects on use cases such as collateral management, shared know your customer (KYC), and Euro tokenization. Now with more than 35 members, including regulators and researchers, LaBChain has become a gateway into the French blockchain ecosystem. "The point was to create a *do* tank, not only a *think* tank," Filali says.

If one mission of the blockchain and cryptoassets program is to support the adoption of the technology, another is to explore potential applications for its business units and clients. Filali assembled an internal team who understood blockchain and its potential impact, including people from the legal, IT, and finance units, and began implementing solutions. Her team and their extended network are now able to develop in-house blockchain products, consult with regulators, and guide other public institutions in

adopting blockchain. Their work has led to partnering with the EU Blockchain Observatory and Forum, and Filali chairing the board of INATBA, the International Association for Trusted Blockchain Applications, since April 2021.

Filali's team is also working on a broader project related to digital identity. Along with the French postal service and two energy companies, Caisse des Dépôts founded a startup called Archipels, which provides document certification services. Energy providers can submit the hash (proof of existence) of their certified bills in Archipels' blockchain. This allows banks or administrators to verify the documents provided by their clients and reduce fraud. Archipels currently holds more than 20 million document hashes, creating and updating entries in its ledger. Filali expects this first service to lead to a larger array of identity verification services, such as digital wallets.

Each of these initiatives required heavy coordination between Caisse des Dépôts and French government ministries, business associations, and banks. Filali says any large-scale blockchain project is likely to interact with such institutions, and building an eager coalition of partners is critical. "Sponsorship by our top management was really important for us to grow," she notes.

Building such partnerships may be getting easier as blockchain continues to mature. In 2019 and 2021, the French parliament passed a series of cryptocurrency regulations. These require crypto-services companies to register with financial regulators and comply with anti–money laundering and KYC rules, among other obligations. In a way, Filali says, this has given crypto and blockchain greater legitimacy. Now, institutions that were previously skeptical are looking for ways to engage with these digital assets and exploring concrete use cases in tokenization and self-sovereign identity.

"It's like the planets aligned," Filali says. "We have the energy. We have the competencies. And people understand that if you don't act now, you may miss your opportunity."

The blockchain is forever for one jeweler

Chow Tai Fook, a Hong Kong–based jeweler, is one of the largest diamond sellers in the world. By definition, the company buys and sells physical assets—but that doesn't mean it can't take advantage of emerging digital tools. It currently operates digital sales and marketing platforms, utilizes customer data analytics, and automates much of its production lines. Now it's adding blockchain to its digital portfolio.

One of the main value propositions of Chow Tai Fook's products is the fact that it sells diamonds that are certified by the

Gemological Institute of America (GIA) and that meet the requirements of the United Nations' Kimberly Process, which establishes guidelines for ethically sourcing diamonds. The problem is that less scrupulous sellers regularly skirt these standards, allowing them to sell diamonds for lower prices, and consumers have trouble telling the difference.

This is what led Chow Tai Fook to establish a blockchain that digitizes all of its diamonds' certification information. After cutting and polishing each diamond, the jeweler laser engraves it with a serial number that references a specific entry in a two-party blockchain ledger maintained by Chow Tai Fook and GIA. This preserves an immutable digital record of the diamond's most important information, including provenance and grade. Customers can bring the diamond into a jeweler to have them look up the serial number and associated record, and then access this record through a dedicated mobile application.

"That's how we protect our customers," says Jade Tin Hei Lee, general manager of business analytics and technology applications at Chow Tai Fook Jewellery Group. "With blockchain, they have full transparency into the journey and the quality of their diamond."[13]

Putting this information on the blockchain also helps Chow Tai Fook with its own internal processes. The company has over 5,000 individual jewelry stores, around 65% of which are owned and operated by franchisees. Together, these stores process around half a million diamonds each year, with most diamonds of 0.3 carats or above coming with their own certifications. Matching every diamond that passed through each of these stores to their certifications used to be a more difficult process. Now it's as simple as matching a serial number on a diamond to a blockchain ledger entry.

The company is looking to extend its use of blockchain to ease financial transactions. Franchisees sometimes require bank financing to cover the cost of inventory purchases, and banks need to see information about a store's sales, revenue, and other performance factors before giving that financing. Chow Tai Fook is currently looking into how it can put a franchisee's data into a blockchain ledger to speed up the process and help stores acquire the inventory they need when they need it.

"We aim to use blockchain to store that performance information so the banks can easily verify it," Lee says. "We hope this can help franchises operate more efficiently."[14]

Diamonds are a highly illiquid asset. They have substantial value but can be harder to buy, sell, and trade than assets such as cash or stocks. But Lee says creating a digital record of their value helps decrease some of the challenges. It also helps attract a younger generation of buyers, who are more likely to trust digital certifications. Meeting the expectations of

this younger, more digitally savvy customer base is a key priority for the company.

"Even though Chow Tai Fook is a 92-year-old company operating in an industry that's even older, it's important to leverage technologies like blockchain to take advantage of emerging opportunities," says Lee. "We're an old company, but we keep innovating over the decades."

How blockchain went from mystery to mainstream at the US Treasury

The US federal government is committed to tracking every dollar it spends, more so than most typical enterprises. Transparency and accountability are paramount when dealing with taxpayer money. For that reason, the Treasury Department is investigating how blockchain may enable a new generation of more automated record keeping.

Each year, various federal agencies send out billions of dollars in grants. Recipients of these grants often use the money to make their own grants to smaller subgrantees. Every penny must be tracked as it passes through each organization. Historically, this has meant a large amount of reporting and paperwork for grant recipients.

To alleviate some of this burden, the US Department of Treasury's Bureau of Fiscal Services is working to develop a blockchain solution to make the process of distributing grants and tracking the flow of money simpler. The project essentially turns grant payments into digital tokens that represent actual money. Recipients can either redeem the token with government agencies for cash or divide it up and distribute to subgrantees, who also would be able to turn their token into actual money. Along the way, each token transaction updates a blockchain ledger with information about how much money was transferred and for what purpose.

Most of this information is automatically generated, which means the process stands to replace much of the reporting that grantees and subgrantees must do when receiving government funding. Some estimates suggest that research institutions spend upwards of 44% of their time on administrative tasks such as reporting. Using blockchain to track payments could eliminate much of this.

"We're able to attach the funding element with all that grant information," says Craig Fischer, innovation program manager at the Department of the Treasury.[15] "We know who it's from, what it's for, [and] the intent of the funding. It has that entire history baked in. With blockchain, recording is reporting."

The project is still at the proof-of-concept (POC) stage. Right now, the application can tokenize grants and record grants and subgrants in a blockchain ledger. It needs the final piece: an all-purpose API connecting the blockchain ledger to legacy downstream payment systems.

The grant payment project builds on other blockchain POCs Fischer and his team have already run. The first was a project to use blockchain to track phones used by employees. The second managed software licenses to track which employees were still actively using a license and which licenses could be restocked.

Fischer says each of these initiatives has been geared toward raising the profile of blockchain within the department and demonstrating that it has use cases beyond cryptocurrency. There are several challenges to using blockchain in a government agency.

For one thing, Fischer says he's not aware of any other mature blockchain payment projects in the federal government, so his team must design and develop supporting processes like access control and security standards.

But Fischer is confident that their POCs are building real traction for the use of blockchain across the federal government. Initially, the hardest thing was educating people on what blockchain is. Now people are starting to get it and he can focus on demonstrating value.

"It used to be important to say, 'I'm using blockchain to solve this problem.' Now it's just 'I'm solving this problem,'" says Fischer.

MY TAKE

Andre Luckow

PhD, head of emerging technologies, BMW Group IT

Two decades of working and studying emerging technologies have taught me to recognize the difference between hype and hope—between the technologies that are truly transformative and those that are not.

In 2018, I was asked to consider potential use cases for blockchain, when it was at the peak of its hype cycle. Naturally, I approached the topic with a dose of healthy skepticism. But as our organization narrowed down the possibilities, we found the right use case for transformation.

I see business problems through the lens of data, and one part of the BMW Group's operations that needed better data was our complex supply chain. We produce approximately 10,000 vehicles a day in 31 plants across 15 countries, leveraging a complex global supplier network. Not so long ago, we still relied on spreadsheets and email. Fraud, limited visibility into second-tier suppliers, and

mismatch of supply and demand were common issues that had the potential to cause production disruption and quality issues. My team started with a proof of concept that allowed the BMW Group and a handful of suppliers to share supply chain data more easily over a blockchain. Real-time visibility, shared among all supply chain members, prevented overstocking and shortages. The transparency not only benefited us with more information about part origins but also enabled our suppliers to uncover improvement opportunities.

After displaying our prototype to our leadership and supplier partners, the BMW Group saw the clear business opportunity and invested in scaling up our blockchain work to more suppliers. The initiative, formally known as PartChain, has enabled nearly seamless transparency and impacted broader data-sharing initiatives such as the Catena-X, Automotive Network e.V. Catena-X creates a collaborative data ecosystem along the automotive value chain, enabling businesses such as OEMs, small and medium enterprises, and recycling companies to take full advantages of a secure data-based economy. By all accounts, the technology has proven fruitful in inspiring initiatives that accelerate data visibility across our value chain.

We are also exploring use cases for blockchain that begin to improve the driver experience. Despite our advances in manufacturing and supply chain, selling or renting cars to consumers is still a fraught, paper-laden process. We recently partnered with the German government to use blockchain as a means of federating driver's licenses and simplifying the purchase process. Self-sovereign identity allows German citizens to verify their licenses frequently with ride-sharing or insurance companies with minimal friction and maximal security, while providing sellers an easy way to reduce identity fraud. In the not-so-distant future, we expect buying a car could be as easy as scanning a QR code.

Looking back on the hype around blockchain in 2018 and the progress the BMW Group has made since, two things are clear. One, blockchain is transformative, and one day we will be using blockchain-based technologies without even realizing it because of the potential they have to build better business processes and customer experiences. Two, the transformation may take longer than anyone anticipated. Businesses need to adopt broader thinking as to which new markets or ecosystems can be supported and simplified through blockchain; they need to ask the right data-driven questions to find their appropriate use cases. If we push the technology forward from all sides, we're bound to see even more great ideas surface.

EXECUTIVE PERSPECTIVES

STRATEGY

CEOs have the unique opportunity to work with their IT leaders to understand the art of the possible when it comes to blockchain technologies. Today's advances in blockchain technology are akin to the adoption of TCP/IP protocols for the internet 30 years ago. Though broad understanding of blockchain technology is still limited, the possibilities for impacting business models are vast. Just as databases enabled business process reengineering within organizations, DLTs enable streamlined processes between organizations. CEOs need to decide how early they want to be on the adoption curve.

FINANCE

Although many CFOs have acknowledged the theoretical utility of blockchain and other digital ledger technologies, they have been hesitant when it comes to full-scale adoption. CFOs can use agile techniques to test DLT use cases to become more confident in their efficacy and safety. They can work closely with IT leaders to identify test cases, deploy experiments, and monitor results. Once use cases are successful, organizations can review the regulatory and financial risks before scaling to enterprise and inter-party adoption.

RISK

Enterprise adoption of blockchain is not yet widespread, and an understanding of the technology's risks is still nascent. Chief risk officers should collaborate with IT to improve their organization's readiness for emerging tech. They can build road maps for adoption and identify use cases for blockchain, as well as proactively reduce risks. New applications of cryptography, for example, can vastly improve the efficiency and reliability of transaction verification, while blockchain-based digital identity solutions can enhance the security of sensitive transactions. Moreover, the blueprints used for blockchain readiness can be applied to further adoption of emerging tech, such as quantum computing.

ARE YOU READY?

KEY QUESTIONS

1 What new delivery models, revenue streams, or business process improvements could be unlocked by maturing blockchain and DLT platforms and standards?

2 How could decentralization improve the way you communicate, collaborate, and exchange data with other organizations or ecosystem partners?

3 Can you identify opportunities to build or increase customer trust by using blockchain to ensure the transparency and traceability of product or service development, creation, and distribution?

LEARN MORE

2021 Global Blockchain Survey
Check out the latest insights where financial leaders increasingly see digital assets as the future.

The rise of using cryptocurrency
Consider the benefits of crypto and other digital assets for investment, operational, and transactional purposes.

Blockchain to blockchains
See how coordination and integration of multiple blockchains can work together across the value chain.

AUTHORS

Our insights can help you take advantage of emerging trends. If you're looking for fresh ideas to address your challenges, let's talk.

Wendy Henry
Government & Public Services Blockchain leader
Deloitte Consulting LLP
wehenry@deloitte.com

Linda Pawczuk
Global Blockchain & Digital Assets leader
Deloitte Consulting LLP
lpawczuk@deloitte.com

SENIOR CONTRIBUTORS

Hiroki Akahoshi
Director, Deloitte Tohmatsu Consulting LLC

Marie-Line Ricard
Partner,
Deloitte France

Tyler Welmans
Director,
Deloitte MCS Limited

Claudina Castro Tanco
Senior manager,
Deloitte Consulting LLP

Jesus Pena Garcia
Senior manager,
Deloitte Luxembourg

Wiktor Niesiobędzki
Specialist lead,
Deloitte Poland

Ruchir Dalmia
Senior consultant,
Deloitte MCS Limited

Lily Pencheva
Senior consultant,
Deloitte MCS Limited

Nicklas Urban
Senior consultant,
Deloitte Consulting GmbH

ENDNOTES

1. Martha Bennett and Charlie Dai, "Predictions 2021: Blockchain," Forrester, October 28, 2020.
2. Deloitte Insights, *Blockchain to blockchains: Broad adoption and integration enter the realm of the possible—Tech Trends 2018*, December 5, 2017.
3. John Schmidt, "Bitcoin's energy usage, explained," *Forbes*, June 7, 2021.
4. KBV Research, *Global blockchain technology market by type (public, private and hybrid), by component (infrastructure & protocols, application & solution and middleware), by enterprise size (large enterprises and small & medium enterprises), by industry vertical (BFSI, IT & telecom, healthcare, retail & ecommerce, government & defense, media & entertainment, manufacturing and others), by regional outlook: Industry analysis report and forecast, 2021–2027*, May 2021.
5. Linda Pawczuk, Richard Walker, and Claudina Castro Tanco, *Deloitte's 2021 Global Blockchain Survey: A new age of digital assets*, Deloitte Insights, 2021.
6. Yahoo.com, "Global Blockchain Market (2021 to 2026) - by Component, Provider, Type, Organization Size, Deployment, Application, Industry and Geography," accessed November 29, 2021.
7. Fortunebusinessinsights.com, "Blockchain Market Size, Share & Covid-19 Impact Analysis, 2021-2028," accessed November 29, 2021.
8. MITRE, *Assessing the potential to improve grants management using blockchain technology*, 2019.
9. VISA, *NFTs: Engaging today's fans in crypto and commerce*, accessed November 2021.
10. 101 Blockchains, "Real world blockchain use cases—46 blockchain applications," July 6, 2018.
11. Rachel Wolfson, "Game time? Microsoft adopts Ethereum blockchain for gaming royalties," *Cointelegraph*, December 18, 2020.
12. Nadia Filali (head of the blockchain and cryptoassets program, Caisse des Dépôts), interview, October 15, 2021.
13. Jade Tin Hei Lee (general manager of business analytics and technology applications, Chow Tai Fook Jewellery Group), phone interview, September 23, 2021.
14. Ibid.
15. Craig Fischer (innovation program manager at the US Department of the Treasury), interview, October 29, 2021.

IT, disrupt thyself: Automating at scale

AUTOMATE INFRASTRUCTURE

Manage your infrastructure via code, not keyboard.

AUTOMATE SYSTEM AND SOFTWARE MANAGEMENT

Manage your systems, tools, and software via code, not keyboard.

OPTIMIZE YOUR AUTOMATION

Implement machine learning for key areas. (Identify likely outages.)

TREND 4

IT, disrupt thyself: Automating at scale

Future-forward IT organizations are modernizing the "IT back office" to a proactive model of self-service and engineered automation

There is still an enormous amount of repeatable work done by people in many established organizations. Think of administration, monitoring, reviews, and responding to tickets among other tasks. Over the last decade, cloud vendors have demonstrated how automating processes that remove repetitive work can help increase overall efficiency. Automated processes are consistent and auditable, which can help reduce errors and improve quality. It can also free skilled tech talent to focus on higher value-added tasks.

IT leaders, for various reasons, have been slow to pursue these opportunities. This, however, is beginning to change. In what we recognize as an emerging trend, some CIOs are disrupting their organizations and the army of technologists that currently execute many manual tasks and handoffs across systems, architecture, development, and deployment.

Beyond leveraging investments made by cloud providers to accelerate their journeys, CIOs are following the cloud providers' playbook to identify and standardize processes. They are attacking opportunities in infrastructure, software components, security, and applications. Once their enhancements mature, CIOs and their teams optimize the new service delivery and automation using advanced techniques such as AI and ML.

Early participants in this trend have already seen gains in efficiency and lower labor costs. In a recent survey of IT and engineering leaders, 74% of respondents said that automation has helped their workforce work more efficiently. Fifty-nine percent reported cost reductions of up to 30% on teams that have embraced process automation.[1] Add to this noticeable increases in quality and security, and it becomes clear why 95% of respondents are prioritizing process automation, with 21% saying it's a high priority.[2]

The pace of change only continues to increase. The business is asking for more, and they want it more quickly than ever before. The talent market is white hot, with growing demand for advanced skill sets (that are in perpetually short supply.) Everyone is trying to do more with less.

The time to (finally) disrupt IT is now.

Disruptive journeys

The journey from manual to automated activities isn't new. Indeed, in previous *Tech Trends* reports, we have examined this transition in areas such as cybersecurity, advanced networking, and the dynamic provisioning of hardware and software. So, what is different this year? Simply put, competition. The pandemic is upending the labor market. Perhaps more importantly, it's in digital natives' DNA to push automation to its limits. Hence, startups can achieve greater scalability, reliability, resilience, and efficiency at lower costs than their established counterparts. They hold an additional advantage in that they aren't held back by technical debt or organizational compromises that require handoffs and manual interventions. For digital natives, such old-school actions become a last resort rather than the norm. This approach is fundamentally different from those often taken by established organizations. Today's competitive marketplace requires a more robust IT posture, which can translate into a competitive advantage.

Organizations looking for opportunities to disrupt their status quo can focus their efforts in three areas:

Standardize and automate on-premises infrastructure

The first leg of an automation journey involves enabling all infrastructure and management functions to be controlled by code. Programmatic control of resources makes it possible to apply policies consistently and to store previously manual configurations in automated code and configuration files. These solutions require deploying some mix of compute (containers, virtualized servers, and functions), networking (software-defined), and storage.

For automation to scale, processes must be executed consistently across the enterprise. However, if you look at the operational landscapes of many organizations today, you will find a mixed bag of processes, applications, and workarounds. When processes work in one fashion on server A and another on server B; when environments do not have parity; or when networks behave differently, then operations become more costly and inefficient.

If this sounds familiar, consider creating a standard, common approach to developing, deploying, and maintaining your solutions and components. Cloud vendors realized early on that the more you can programmatically control resources, the easier it becomes to treat environments as a program to be managed. Many of today's infrastructure-as-code platforms trace their roots to early cloud-based automation initiatives.

As organizations explored infrastructure-as-code, they recognized they could also deploy security-as-code or operations-as-code, controlling them all with configuration or code files. The goal of "as-code" is to push toward an environment in which everything—even bespoke systems—aligns on a set of optimized rules. With rules in place, a single engineer can control a large pool of resources that would have taken several administrators to manage. This frees infrastructure teams to work like the cloud providers: automating, taking advantage of opportunities for self-service, and getting out of the way.[3]

As organizations streamline operations and management with automation, they should also revisit their initiation processes. Historically, creating new infrastructure involved elaborate procurement exercises with escalating approval levels. In today's world, adding another virtual instance may not warrant any level of prior approvals. Identifying and automating (or eliminating) similar handoffs and approvals that made sense in a legacy environment can help streamline operations, augment developer productivity, and provide much sought-after organizational agility.

When approached methodically and strategically, automation can deliver significant economies of scale. It offers other benefits as well:

- **Greater accuracy.** Individuals will no longer be subjectively interpreting documents, queries, and forms.
- **Increased security and resilience.** Rules will be applied more consistently. It's worth noting that a nascent "security-as-code" trend is gaining momentum.
- **Improved reliability.** Problems fixed in the code typically won't reoccur.

We offer a word of warning for those using the providers' "as code" services. Make sure you have organized your processes and operations to get the most out of those capabilities. If you don't, you may reproduce existing limitations in a modern environment.

Standardize and automate software, management tools, and applications

Leading-edge IT organizations no longer manage infrastructure; they now develop code that manages infrastructure, an approach that can boost scalability, efficiency, and consistency. This same approach can apply to software components, management tools, and a variety of applications. Modern IT organizations manage software code that, in turn, manages aspects of development, maintenance, operations, and security. Ultimately, it is easier to manage a single piece of code than an array of manually configured solutions. For example, infrastructure-as-code enables us to bring the agility of software development to infrastructure management. From a deployment perspective, it is possible to manage full-stack solutions rather than separate components that several teams must coordinate.

Like infrastructure, a few on-premises software components are prime candidates for automating. For example, database management, integration tools, security, systems management, and O/S patching can be easily virtualized and abstracted.

For organizations using cloud infrastructure, vendors offer an expanding menu of platform-as-a-service (PaaS) options that feature enhanced automation, programming interfaces, integrated middleware, and management capabilities. Maturing PaaS offerings may also provide enhanced developer self-service, programming interfaces, and more tightly integrated middleware and management capabilities.

How can you decide where to start? First, identify the "user journeys" of those trying to deliver functionality to end users, and the points of friction these users encounter. Ruthlessly prune unnecessary approvals and handoffs and then automate or create self-service options for the steps that stand between developed code and production deployments. Finally, once your automation journey is underway, old performance metrics may no longer apply. It's important at this point to incentivize an "automation culture" by defining metrics for the organization you want to become.

Optimize automation with ML and rules

Typically, a first pass at automation is rules-based. For example, "if process x doesn't respond, restart the process." Over time, IT staff members can identify issues that cause outages and malfunctions and optimize automation tools to address them,

just as cloud providers demonstrated a decade ago. Eventually, you can move beyond rules-based to machine learning–based automation. An automation journey that begins immaturely can subsequently grow in terms of sophistication.

Many types of ML—predictive, capacity modeling, action response, outage recovery, among others—support different IT activities. Yet for most organizations, identifying outages early and harnessing predictive modeling to prevent future outages is a top ML priority. By focusing on these areas, ML-enabled teams can measurably improve uptime and decrease outage severity. Moreover, a growing number of PaaS offerings feature embedded ML capabilities. For example, PaaS offerings often use ML to maintain and optimize routine operations that were previously managed manually by developers, administrators, and engineers. The net effect is that development and operations can run in higher gears.

Another optimization technique involves applying rules consistently. Consider this: Enterprise architecture is a set of decisions around what you can use and how. The resulting rules represent an optimum approach to architecture design and function. As part of your automation journey, consider prioritizing consistency. Do this by methodically embedding these rules into systems and processes across the enterprise. Consistency delivers optimum performance.

The way forward

For CIOs and other leaders who are exploring automation opportunities, time is of the essence. In today's rapid-fire innovation climate, there is not a lot of business value to be found in paying humans to maintain servers and data centers. As CIOs disrupt their IT organizations with automation, there will be ripe opportunities to shift employees' focus from patching, monitoring, and measuring to higher-value engineering activities. More broadly, automation's possibilities extend to areas such as development, deployment, maintenance, and security, thus making it possible to gain efficiency and consistency across more of IT's operations.

The journey from managing things to managing code that manages things won't happen overnight. For example, there may be some cultural resistance from tech workers and the C-suite, or legacy systems may have manually configured components that make automation difficult. Finally, change is hard, even for the nimblest IT teams. People accustomed to handoffs and human-to-human interaction may adapt slowly to self-service and automated provisioning. For organizations just getting started, it may be helpful to create a dedicated team that develops and deploys automation and self-service to standard processes. This team can methodically broaden its approach,

transforming more processes over time as they climb the stack.

Luckily, some needed automation is readily available in the form of cloud-based solutions. The rest is achievable through engineering and a deliberate, consistent focus on building an automated future.

LESSONS FROM THE FRONT LINES

Automating in the cloud unleashes developer agility and speed of innovation

Back in 2015, Capital One stated all new applications would be built and run in the cloud and all existing applications would be migrated to the cloud. This may have seemed like an ambitious goal at the time given the scale of the enterprise's on-premises infrastructure and the fact that it's rare for any business to operate entirely in the cloud. But the financial services firm hit its target, becoming the first US bank to report that it has exited legacy data centers and gone all-in on the public cloud.[4] This has delivered several benefits, but among the most important is the increased opportunity for automation and the rapid scaling that comes with it.

As Capital One was moving more data and applications to the cloud, the technology team members knew they didn't want to simply replicate their existing systems and processes. They wanted to take advantage of the cloud's full range of possibilities for building a more modern technology stack. This included adopting leading trends like microservices, automation, real-time data, and machine learning.

"Compute and storage are just the tip of the iceberg with cloud," says Chris Nims, senior vice president for cloud and productivity engineering in the technology division at Capital One.[5] "If you just forklift your applications to the cloud, you don't get the full range of benefits."

Capital One now increasingly leverages a serverless computing model to make sure developers don't have to worry about finding compute resources, combined with containers to deliver applications, and necessary libraries and other dependencies. The team also built a rules engine that it open-sourced that helps organizations define policies to better manage their cloud environments with automated governance, security, compliance, and efficiency.

All these moving parts may look complicated, but the team found it has led to better uptime. Part of utilizing the modern tech stack means it's able to deploy automated monitoring tools. Machine learning applications monitor real-time

server data and system applications to ensure they're running smoothly and alert technicians to problems before most users notice them.

"The parts have gotten smaller, and we knew the old way of manually doing monitoring wasn't going to scale," says Arjun Dugal, CTO of the financial services division at Capital One.[6] "We've had to reinvent how we monitor our applications ecosystem by leaning on advanced cloud-native monitoring tools and leveraging machine learning–based anomaly detection. Our strategy has paid off—incidents have actually gone down even as the number of potential points of failure has dramatically increased."

Automating infrastructure has made Capital One a more attractive player in the battle for tech talent. Nims says most people who go to school for computer engineering do so because they like the challenge of solving hard problems. When they graduate, they don't want to spend their time seeking approvals, monitoring server performance, or maintaining outdated databases. Automating these things lets engineers spend their time on more impactful projects, which gives Capital One a leg up in hiring. "Great engineers want to work on modern infrastructure," Nims says. "They want to be at the forefront of technology. So much of this goes back to allowing our engineers to spend their time on the most important things."

Improving the job satisfaction of developers isn't just about attracting talent. It's also about business value. Dugal says Capital One employs 11,000 technologists, 85% of whom are developers, so even marginal increases in their agility scales to major benefits for the company.

"This is about getting the mechanics out of the way so they can focus on the highest value things," he says. "Greater developer agility translates directly to a big boost in customer benefits and speed of innovation."

UiPath paves the way to IT automation success

UiPath, a leading provider of robotic process automation (RPA) platforms since 2005, has been enabling customer automation journeys by starting with an ambitious strategic vision for what automation can deliver. It then creates an operating model that ensures automation continuously improves and brings value to customers.[7] According to Jay Snyder, senior vice president of customer strategy and solutions at UiPath: "Automation is empowered and governed by IT but enabled by the business. That's where the chocolate and peanut butter all comes together."

Having helped hundreds of organizations automate business processes, UiPath is increasingly turning its expertise toward the business of IT. According to Eddie O'Brien,

senior vice president of operations and partners, more involvement from senior leaders in IT can help an organization scale its automation efforts within IT departments: "Often, people put their feet in the water with automation, but don't know where to go next. Closer engagement with IT can bring about more digital transformation."

When used properly in IT, says Snyder, teams not only control the automation platform but can also turn it inward to automate IT processes such as ticket creation, license management, or cybersecurity response. Even beyond individual processes, the vision is to enable zero-touch IT by automating high-impact IT services such as DevOps and data management. Snyder's team works with IT departments to create playbooks of automation use cases, prioritizing the highest-volume, lowest-value tasks. Team members also create IT personas, such as a system admin persona, to teach their RPA platform how to accomplish a set of tasks across various business processes or departments, just as an IT employee would. In doing so, an organization's IT staff can focus on performing higher-value tasks or designing further automations. "People often focus on reducing staff through automation, but we've seen that the true benefit is in multiplying productivity," says Snyder.

The result is a cycle of automation that continues growing in IT departments. As more employees are empowered by digital assistants, team members generate more automation ideas, and robots are further incorporated into IT processes. In addition, the AI/ML in the platform analyzes an organization's automations and can recommend improvements or expansions. According to O'Brien, the key to achieving ongoing IT automation is to start with the right strategy in place. The goal is to create end-to-end automation that drives digital and business transformation. Says O'Brien, "When we bring our vision of the fully automated enterprise to fruition, we can have a major impact on the efficiency of IT and how it's managed today."

Automation helps Anthem stay ahead of insurance industry turbulence

Anthem, Inc., provides health insurance to about 40 million people across the United States, and connecting these members to care is its top priority. That's why in recent years the company has reoriented its IT department to serve its member-focused mission by automating large segments of its core infrastructure, allowing engineers to spend time on projects that are closer to business priorities.

"The industry has moved from managing things to building things," says Srinivas Yamujala, staff vice president of the cloud center of excellence at Anthem.[8] "In order for Anthem to stay competitive, we had to be more digital and nimble. In support of our transformation initiatives, our focus has been on end-to-end automation to simplify and expedite delivery of infrastructure services and shared platforms so that we can build and release applications and products more quickly."

One of the areas of focus as part of this journey has been to enable cloud. Anthem was relying on traditional infrastructure delivery based on manual, cumbersome processes to acquire and provision infrastructure, Yamujala says. If onboarding a new customer called for increased server capacity, it could take three to six months to acquire and fully configure the hardware. But now, Anthem has most of its business processes in the cloud, and this formerly months-long process takes as little as two hours. It has developed a patent pending orchestration and provisioning automation platform that is secure and compliant with health care domain regulatory and security policies. This, in turn, has enabled the application development teams to provision resources on demand in minutes.

To support innovation and transformation initiatives, Anthem took its cloud vendor services and hardened them with Anthem's rigorous security protocols. These preconfigured services are assembled into a service catalog, providing application developers with the capability to use several native cloud vendor services that already meet legal and security compliance standards. In the past, each development team wanting to use a particular service would have to build guardrails for these services themselves, resulting in disparate approaches and redundant implementations.

In addition, while working on applications, developers previously had to submit tickets with security teams to open specific firewall ports so that their applications could communicate with other systems and applications. Now, Anthem has baked all that into its automated platform using microservices and APIs. The need for developers to manage cumbersome firewall changes has been minimized, and Anthem is working toward eliminating it altogether using zero-trust capabilities. This has improved its developer community productivity tremendously, which is anticipated to get even better in the future.

"We want to empower our developer community," says Yamujala. "Most of our automation efforts are about simplifying application development and deployment. A lot of automation you see today is about infrastructure as code, but we're going beyond that to

think about what enables developers to address business needs more quickly."

An additional benefit of automating all of this is that it's helped improve system uptime. Maintaining on-premises infrastructure forces engineers to monitor servers and the applications they host. With all the interdependencies between applications and hardware configurations, engineers had a hard time staying ahead of issues, Yamujala says. Now that complexity is handled by cloud services, and system performance has improved.

The move to automate core infrastructure and platforms, as well as aspects of application development and deployment, has had benefits far beyond IT. Yamujala says the broader business is now in a better position to respond quickly to evolving business needs and customer expectations.

"Our ability to respond to changing industry needs, to customer needs, and to sustain business in changing conditions has become even more nimble, agile, and fast," Yamujala says.

OUR TAKE

Bill McDermott

President and CEO of ServiceNow

C.J. Desai

Chief operating officer at ServiceNow

At ServiceNow, we think of our platform as the control tower for digital transformation across the enterprise.

In today's digital world, IT architecture *is* business architecture, and developing a coherent approach to automation across your technology infrastructure has never been more important.

We know this because at ServiceNow, we are "client zero." Everything we put out into the world we use internally first. This helps us see the impact of automation and understand the benefits of coordinating our digital activities. It has also helped us understand how automation needs to work in a modern IT organization, one that supports the digital transformation vision of the entire enterprise.

When our platform started out, we supported prescriptive workflows, and our initial use case was IT service management. Over time, clients began using the platform for other use cases, such as cybersecurity operations, HR onboarding and offboarding, and customer service,

to name a few. And our platform has grown to support machine learning–enabled automation and will soon offer RPA capabilities for systems that lack clean interfaces.

Yet automating discrete front-end processes is not the ultimate objective in any digital transformation effort. The real goal is to clean up the messy middle and back-end systems and integrate islands of automation on the front end. Over the years, businesses have spent billions of dollars making sure their digital front ends and customer experiences shine. Yet many have invested much less in the back-end systems and supporting technologies, which remain replete with manual processes. This slows operations down and minimizes the benefit of great front-end customer experiences.

Customers won't accept this—they want what they want, when they want it. They expect visibility. You may have a great ordering system, but if customers can't track the status of their orders, the overall customer experience is lacking.

This is why we advocate moving away from the older system of record models to a more modern "system of action" approach. You need to connect with your customers throughout the entire sales process, not just on the front end. Manual efforts don't scale. Automation does.

Automation isn't just about meeting customer expectations. It's also important for improving the employee experience. Few workers want to do the same rote tasks every day. This is especially true for developers and engineers, who would rather spend their time solving high-value, complex problems than doing basic system monitoring. At the same time, businesses across industries are struggling to find the talent they need. The talent war is real, and most enterprises are having a hard time keeping up. Automating low-value tasks frees your employees to work on higher-value problems, which is one of the best ways to improve the talent experience and boost retention.

Ultimately, this is all about increasing speed to value. Whether the goal is connecting with your customers or empowering employees to work on higher-value tasks, a coordinated approach to automation helps your business realize gains much more quickly. Once you've automated your operations, the time to value ranges from weeks to months, rather than months to years.

EXECUTIVE PERSPECTIVES

STRATEGY

Automation technology applied to IT promises benefits to efficiency, resilience, and scalability. CEOs should work closely with IT leaders to understand the plans to meet operational and strategic goals. Because the move enables IT staff to focus on more value-added work, leaders can work with CIOs and other tech leaders to refocus and retrain the IT workforce. They can create excitement around personal growth and learning, instead of apprehension around changes to IT, and open new possibilities for technology's role in the organization.

FINANCE

With tech talent in historically high demand, CFOs should welcome the accelerating shift toward automation. Beginning the journey by automating mundane IT activities requires upfront investment of both talent and funding. As IT talent is freed from routine work, increasingly sophisticated automation can be applied with increased resilience and at lower cost. Upskilling and retooling will be required, but the shift to automation opens more options to source diverse IT talent.

RISK

As companies increasingly automate IT, bad actors may look for additional attack vectors. In legacy environments, administrators were trained to bring systems back online after outages and incidents. Without proper planning, automated environments can present challenges. CROs should emphasize resilience when IT processes are being digitized and automated. As organizations automate, they can build in their risk management principles at the outset, using AI to respond more proactively to emergent threats.

ARE YOU READY?

KEY QUESTIONS

1 Which of your infrastructure and management functions currently require manual intervention? Of these, which can you standardize and automate?

2 What is the lowest value activity performed by each of your employees? Can it be automated or eliminated?

3 Which of your automated functions are candidates for optimization? How are you moving beyond rules-based decision-making to explore ML optimizations?

LEARN MORE

NoOps in a serverless world
Read on to see how the hyperautomation of cloud computing has created a NoOps environment to help drive business outcomes.

Enterprise IT: Thriving in disruptive times with cloud and as-a-service
Read the 2021 edition of the Everything-as-a-Service (XaaS) Study and see how adopters are benefiting from the XaaS model.

Digital transformation collection
Explore latest insights driving efficiencies, powering new products and services, and enabling new business models.

AUTHORS

Our insights can help you take advantage of emerging trends. If you're looking for fresh ideas to address your challenges, let's talk.

Kacy Clarke
Cloud architecture go-to-market lead
Deloitte Consulting LLP
kaclarke@deloitte.com

Ken Corless
Cloud engineering managing director
Deloitte Consulting LLP
kcorless@deloitte.com

Glen Rodrigues
Foundry services market leader
Deloitte Consulting LLP
grodrigues@deloitte.com

Lars Cromley
Cloud engineering technology fellow
Deloitte Consulting LLP
lcromley@deloitte.com

SENIOR CONTRIBUTORS

Julien Kopp
Partner,
Deloitte France

Andreas Zachariou
Director,
Deloitte MCS Limited

Alice Doyne
Senior manager,
Deloitte MCS Limited

Kelly McLaurin
Senior manager,
Deloitte Consulting LLP

Naoki Morinaga
Senior manager, Deloitte
Tohmatsu Consulting LLC

João Sanches
Senior manager, Deloitte &
Associados SROC, S.A.

Takashi Torii
Senior manager, Deloitte
Tohmatsu Consulting LLC

Bertrand Polus
Manager, Deloitte Tohmatsu
Consulting LLC

ENDNOTES

1. Salesforce, *IT leaders fueling productivity with process automation*, accessed November 9, 2021.
2. Ibid.
3. David Linthicum et al., *The future of cloud-enabled work infrastructure: Making virtual business infrastructure work*, Deloitte Insights, September 23, 2020.
4. "How Capital One Moved Its Data Analytics to the Cloud," *Harvard Business Review*, February 23, 2021.
5. Chris Nims (senior vice president for cloud and productivity engineering in the technology division, Capital One), interview, October 25, 2021.
6. Arjun Dugal (CTO of the financial services division, Capital One), interview, October 25, 2021.
7. Jay Snyder (SVP customer strategy and solutions, UiPath) and Eddie O'Brien (SVP operations and partners, UiPath), interview, October 27, 2021.
8. Interview with Srinivas Yamujala, staff vice president of cloud center of excellence, Anthem, Inc., November 5, 2021.

Cyber AI: Real defense

PROTECT EXPANDING ATTACK SURFACES

Enterprise vulnerability is increasing as ever more systems and data are exposed online.

BRIDGE THE CYBER TALENT GAP

AI can help enterprises address their chronic shortage of cybersecurity talent.

FIGHT FIRE WITH FIRE

AI-driven security tools will likely be the best defense against emergent AI-driven security threats.

TREND 5

Cyber AI: Real defense

Augmenting security teams with data and machine intelligence

Despite making significant investments in security technologies, organizations continue to struggle with security breaches: Their adversaries are quick to evolve tactics and stay ahead of the technology curve. Humans may soon be overwhelmed by the sheer volume, sophistication, and difficulty of detecting cyberattacks.

People are already challenged to efficiently analyze the data flowing into the security operations center (SOC) from across the security tech stack. This doesn't include the information feeds from network devices, application data, and other inputs across the broader technology stack that are often targets of advanced attackers looking for new vectors or using new malware. And as the enterprise increasingly expands beyond its firewalls, security analysts are charged with protecting a constantly growing attack surface.

Meanwhile, the cost of cybercrime continues to climb; it's expected to double from US$3 trillion in 2015 to US$6 trillion by the end of 2021 and grow to US$10.5 trillion by 2025.[1] The average cost of a single data breach in 2021 was US$4.24 million,[2] a 10% increase from 2019.[3] According to insurer AIG, ransomware claims alone have grown 150% since 2018.[4]

It's time to call for AI backup. Cyber AI can be a force multiplier that enables organizations not only to respond faster than attackers can move, but also to anticipate these moves and react to them in advance. Cyber AI technology and tools are in the early stages of adoption; the global market is expected to grow by US$19 billion between 2021 and 2025.[5]

AI's ability to adaptively learn and detect novel patterns can accelerate detection, containment, and response, easing the burden on SOC analysts and allowing them to be more proactive. Bonus: It can help organizations prepare for the eventual development of AI-driven cybercrimes.

Expanding enterprise attack surfaces

Organizations' attack surfaces are exponentially expanding. As discussed in *The tech stack goes physical*, the adoption of 5G networks and an increase in network connections, together with a more distributed workforce and a broadening partner ecosystem, may present new risks. They're exposing the enterprise outside of its firewalls and pushing it into customer devices, employee homes, and partner networks.

More remote workers. Before COVID-19, only about 6% of employees worked from home. In May 2020, about 35% of them did.[6] In the first six weeks of the 2020 lockdown, the percentage of attacks on home-based workers increased fivefold from 12% to 60%.[7] One survey found that 51% of respondents saw an increase in email phishing after shifting to a remote working model.[8]

For many workers, remote work is expected to remain the rule, not the exception, providing cybercriminals with many new opportunities. For example, outside of the safety of corporate firewalls and web security gateways, remote workers are easier to target. They rely on home networks and VPN connections and often use unsecured devices to access cloud-based apps and data. And legacy on-premises security equipment is typically designed to support enterprise-grade networks, not home-based internet access.

As the enterprise extends into its employees' homes, user behavior and data activity become more diverse and deviate from previous norms. With employees logging in from atypical locations and devices at unusual times, it can be more challenging to identify anomalous behaviors, potentially leading to an increase in false positives.

Increase in network-connected devices. 5G, IoT, Wi-Fi 6, and other networking advances are driving an increase in network-connected devices. When seeking a soft attack vector, cybercriminals will be able to choose from a growing number of network-connected physical assets—29.3 billion by 2023, according to one estimate.[9]

The unprecedented number of devices connected to these networks produce data that needs to be processed and secured, contributing to the data logjam in the SOC. It can be challenging to keep track of and manage active assets, their purpose, and their expected behavior, especially when they're managed by service orchestrators.

Rather than being centrally located and controlled, many of these devices are spread across various remote locations, operating in multiple edge environments where they collect data to send back to

the enterprise. Without proper security precautions, devices can be compromised and continue to appear to operate normally on the network, essentially becoming intruder-controlled bots that can release malicious code or conduct swarm-based attacks.

It can be challenging to keep track of and manage active assets, their purpose, and their expected behavior, especially when they're managed by service orchestrators.

Broader ecosystem of third-party partners. An increasingly global supply chain and hosted data, infrastructure, and services have long contributed to third-party risk. And as more and more organizations integrate data with third-party applications, APIs are a growing security concern. Gartner predicts that by 2022, API abuses will become the enterprise's most frequent attack vector.[10]

Third-party breaches are growing in complexity. Five years ago, an intruder might use widely available malware to target specific computer systems, gain contractor credentials, and steal customer data—messy, to be sure, but with a clear source and the ability to monitor and remediate the damage.

Such an attack pales in comparison to today's sophisticated intrusions, in which information stolen from one company can be used to compromise thousands of its customers and suppliers. Supply chain attacks can do the same by exploiting the least-secure embedded components of complex supply networks. A breach with no boundaries can be nearly impossible to monitor and remediate, with active theft potentially continuing for many years.

Adoption of 5G networks. 5G is expected to completely transform enterprise networks with new connections, capabilities, and services. But the shift to 5G's mix of hardware- and distributed, software-defined networks, open architectures, and virtualized infrastructure will create new vulnerabilities and a larger attack surface, which will require more dynamic cyber protection.

5G networks can support up to a million connected devices per square kilometer—compared to only 100,000 for 4G networks[11]—enabling highly scalable and densely connected environments of devices. By 2025, market watchers predict there will be 1.8 billion

5G mobile connections (excluding IoT), up from 500 million in 2021;[12] and about 3.7 billion cellular IoT connections, up from about 1.7 million in 2020.[13]

As public 5G networks expand, organizations in government, automotive, manufacturing, mining, energy, and other sectors have also begun to invest in private 5G networks that meet enterprise requirements for lower latency, data privacy, and secure wireless connectivity. From autonomous vehicles and drones to smart factory devices and mobile phones, an entire ecosystem of public and private 5G network–connected devices, applications, and services will create additional potential entry points for hackers. Each asset will need to be configured to meet specific security requirements. And with the increasing variety of devices, the network becomes more heterogenous and more challenging to monitor and protect.

AI defense against today's cyberthreats

Expanding attack surfaces and the escalating severity and complexity of cyberthreats are exacerbated by a chronic shortage of cybersecurity talent. Employment in the field would have to grow by approximately 89% to eliminate the estimated global shortage of more than 3 million cybersecurity professionals.[14] AI can help fill this gap.

Accelerated threat detection. Threat detection was one of the earliest applications of cyber AI. It can augment existing attack surface management techniques to reduce noise and allow scarce security professionals to zero in on the strongest signals and indicators of compromise. It can also make decisions and take action more rapidly and focus on more strategic activities.

Advanced analytics and machine learning platforms can quickly sift through the high volume of data generated by security tools, identify deviations from the norm, evaluate the data from the thousands of new connected assets that are flooding the network, and be trained to distinguish between legitimate and malicious files, connections, devices, and users.

AI-driven network and asset mapping and visualization platforms can provide a real-time understanding of an expanding enterprise attack surface. They can identify and categorize active assets, including containerized assets, which can provide visibility into rogue asset behavior. Supply chain risk management software incorporating AI and machine learning can automate the processes of monitoring physical and digital supply chain environments and tracking the way assets are composed and linked.

Force multiplier in containment and response. AI can also serve as a force multiplier that helps security teams automate time-consuming activities and streamline containment and response. Consider machine learning, deep learning, natural language processing, reinforcement learning, knowledge representation, and other AI approaches. When paired with automated evaluation and decision-making, AI can help analysts manage an escalating number of increasingly complex security threats and achieve scale.

For example, like its predecessors, 5G is vulnerable to jamming attacks, in which attackers deliberately interfere with signal transfer. Researchers from the Commonwealth Cyber Initiatives at Virginia Tech and Deloitte, who are collaborating to understand 5G network security design and implementation, are working to identify low-level signal jamming before it brings down the network. By implementing an AI-based interference scheme and machine learning models, a real-time vulnerability assessment system was developed that could detect the presence of low-level signal interference and classify jamming patterns.[15]

Automation can help maximize AI's impact and shrink the time between detection and remediation. SOC automation platforms embedded with AI and machine learning can take autonomous, preventative action—for example, blocking access to certain data—and escalate issues to the SOC for further evaluation. When layered on top of the API management solutions that control API access, machine learning models trained on user access patterns can inspect all API traffic to uncover, report on, and act on anomalies in real time.

Proactive security posture. Properly trained AI can enable a more proactive security posture and promote cyber resilience, allowing organizations to stay in operation even when under attack and reducing the amount of time an adversary is in the environment.

For example, context-rich user behavior analytics can be combined with unsupervised machine learning algorithms to automatically examine user activities; recognize typical patterns in network activity or data access; identify, evaluate, and flag anomalies (and disregard false alarms); and decide if response or intervention is warranted. And by feeding intelligence to human security specialists and enabling them to actively engage in adversary pursuit, AI enables proactive threat hunting.

Organizations can leverage AI and machine learning to automate areas such as security policy configuration, compliance monitoring, and threat and vulnerability detection and response. For instance, machine learning–

driven privileged access management platforms can automatically develop and maintain security policies that help enforce zero-trust security models. By analyzing network traffic patterns, these models can distinguish between legitimate and malicious connections and make recommendations on how to segment the network to protect applications and workloads.

Pairing vulnerability analysis and reinforcement learning, security specialists can generate attack graphs that model the structure of complex networks and reveal optimal attack routes, resulting in a better understanding of network vulnerabilities and reducing the number of staff required to conduct the testing. Similarly, cyberattack simulation tools can continuously mimic the tactics and procedures of advanced threats to highlight infrastructure vulnerabilities and routes for potential attack.

Evolving the role of human security analysts. In one survey of security analysts, 40% said their biggest pain point was too many alerts; 47% said it was hard to know which alerts to prioritize for incident response.[16] Another survey found that analysts increasingly believed their role was to reduce alert investigation time and the volume of alerts, rather than to analyze and remediate security threats. More than three-quarters of respondents reported an analyst turnover rate of more than 10%, with nearly half saying the rate was between 10% and 25%.[17]

AI can't replace human security professionals, but it can enhance their work and potentially lead to more job satisfaction. In the average SOC, AI and automation could eliminate the tedious functions of Tier 1 and Tier 2 analysts. (Tier 1 evaluates incoming data and decides to escalate problems, and Tier 2 responds to trouble tickets, assesses the scope of each threat, determines response and remediation actions, and escalates when required.) These analysts could be trained to function in more strategic roles that are more challenging to hire for, such as higher-level Tier 2 analysts and Tier 3 analysts who handle the thorniest security challenges and focus on proactively identifying and monitoring threats and vulnerabilities.

A table-stakes weapon against future AI-driven cybercrimes

The same features that make AI a valuable weapon against security threats—speedy data analysis, event processing, anomaly detection, continuous learning, and predictive intelligence—can also be manipulated by criminals to develop new or more effective attacks and detect system weaknesses.

For example, researchers have used generative adversarial networks—two

neural networks that compete against each other to create datasets similar to training data—to successfully crack millions of passwords.[18] Similarly, an open-source, deep learning language model known as GPT-3 can learn the nuances of behavior and language. It could be used by cybercriminals to impersonate trusted users and make it nearly impossible to distinguish between genuine and fraudulent email and other communications.[19] Phishing attacks could become far more contextual and believable.[20]

Advanced adversaries can already infiltrate a network and maintain a long-term presence without being detected, typically moving slowly and discreetly, with specific targets. Add AI malware to the mix, and these intruders could learn how to quickly disguise themselves and evade detection while compromising many users and rapidly identifying valuable datasets.[21]

Similarly, an open-source, deep learning language model known as GPT-3 can learn the nuances of behavior and language.

Organizations can help prevent such intrusions by fighting fire with fire: With enough data, AI-driven security tools can effectively anticipate and counter AI-driven threats in real time. For example, security pros could leverage the same technique that researchers used to crack passwords to measure password strength or generate decoy passwords to help detect breaches.[22] And contextual machine learning can be used to understand email users' behaviors, relationships, and time patterns to dynamically detect abnormal or risky user behavior.[23]

The way forward

Humans and AI have been collaborating to detect and prevent breaches for some time, although many organizations are still in the early stages of using cyber AI. But as attack surfaces and exposure outside of traditional enterprise networks continue to grow, AI offers more.

Approaches such as machine learning, natural language processing, and neural networks can help security analysts distinguish signal from noise. Using pattern recognition, supervised and unsupervised machine learning algorithms, and predictive and behavioral analytics, AI can help identify and repel attacks and automatically detect abnormal user behavior, allocation of network resources, or other anomalies. AI can be used to secure both on-premises architecture and enterprise cloud services,

although securing workloads and resources in the cloud is typically less challenging than in legacy on-premises environments.

On its own, AI (or any other technology, for that matter) isn't going to solve today's or tomorrow's complex security challenges. AI's ability to identify patterns and adaptively learn in real time as events warrant can accelerate detection, containment, and response; help reduce the heavy load on SOC analysts; and enable them to be more proactive. These workers will likely remain in high demand, but AI will change their roles. Organizations likely will need to reskill and retrain analysts to help change their focus from triaging alerts and other lower-level skills to more strategic, proactive activities. Finally, as the elements of AI- and machine learning–driven security threats begin to emerge, AI can help security teams prepare for the eventual development of AI-driven cybercrimes.

LESSONS FROM THE FRONT LINES

Sapper Labs fights software with software

To help Canadian and US military, government, and critical infrastructure operators solve security challenges, Sapper Labs Cyber Solutions provides cybersecurity thought leadership, intelligence, R&D, implementation, operational security platforms, and training support to solve complex problems. AI is an increasingly important tool in Sapper Labs' technology toolkit.

The Ottawa-based cyber defense firm—which takes its name from the military term for combat engineers who support ground troops through surveillance, scouting, defense engineering, and other proactive defensive activities—starts its projects with the premise that every network, system, and capability is already compromised, and that organizations simply don't have the human resources to defend against or combat this. "The growth of the talent pipeline is not keeping pace with either the growth of the attack surface or the expansion of business and government innovation agendas, so we can't produce enough talent to protect our institutions and assets," says Al Dillon, Sapper Labs' cofounder and CEO. "That's where AI comes in for an assist."[24]

To that end, Sapper Labs is working with several Canadian and US security, defense, and intelligence organizations to create AI systems that aim to flex in real time with evolving threat tactics and procedures of our adversaries. These systems can do much more than inform decisions; they can learn how to defend themselves against threats, regardless of human engagement. "Today, cyber defenses that use machine learning, AI, and automation focus primarily on human-led cyber engagement," says Dillon. "Because of the pace of today's innovation and the proliferation of networks and devices, especially outside of the organization, we're going to need embedded automated system capabilities."

Dillon says the collective goal for national security and defense organizations and other public and private sector organizations should be to shift toward military-grade, software-led engagement: AI-driven software defending—and fighting back against—AI-enabled adversaries. "We're all under threat of attack by nation-state actors and other bad actors with equivalent intent, expertise, and tools," he explains.

For example, Sapper Labs and government agencies are developing a multilayered threat detection system that fuses information and data feeds from a variety of sources, known as all-source intelligence—from satellite-, land-, and sea-based sensors to digital sources such as social media and other public and private network information. Examining this data in the traditional manner might take human-led security teams months or even years. Automating the process of synthesizing this data and intelligence and applying algorithms to it enables evaluation and decision-making to take place 10 or even 15 times faster than with conventional methods. Within three years, Dillon expects cyber AI and automation technologies to have advanced so far that they will be able to evaluate intelligence, reach a conclusion, and make a decision 50 times faster than in the past.

Therein, says Dillon, lies one of cyber AI's toughest problems. "Overcoming the people, societal, and cultural challenges to cyber AI will be far more difficult than solving technology problems," he says. "The biggest hill to climb will be getting people to trust decisions made by AI when they're more comfortable with decisions made by human leaders, even if it takes 50 times longer to get those decisions."

Education is one of the keys to building this trust. Through partnerships with other private companies, public-sector organizations, and academic institutions, Sapper Labs is working to help build awareness of automated cybersecurity more broadly. "We're in an exciting transition in terms of technology adoption and innovation, but it's alarming that we don't fully understand the societal impact with regards to defending national security, personal data, intellectual property, and other crown jewels," Dillon says. "We have to internalize that AI-enabled security platforms may become the only way that we can stay ahead of the bad actors."

MY TAKE

Mike Chapple

Information security leader and IT, analytics, and operations teaching professor, University of Notre Dame

Over the last year, the nature of cybersecurity attacks has transformed.

Previously, one of the main concerns for an organization would have been ransomware attacks, wherein bad actors would gain access to enterprise data through phishing or internet malware, and then encrypt that data to hold it for ransom. Such attacks were opportunistic because criminals would take advantage of whoever fell prey to malware, and they didn't always succeed if organizations were prepared with data backups.

The stakes are now higher because bad actors are engaging in organized crime, akin to cyberwarfare by nation-states. We've seen hospitals targeted during COVID-19 outbreaks, pipelines unable to deliver fuel, and other highly targeted attacks. The bad actors' new paradigm is to present two extortion threats on stolen enterprise data: holding the data hostage and threatening to leak sensitive information, including customer records and intellectual property. Such threats are especially salient for large organizations,

which have the money and data desired by cybercriminals. Moreover, the attack surface for such crimes is ever-expanding as trends such as the adoption of 5G mobile networks and work-from-home policies push enterprise technology beyond its traditional borders.

How can organizations respond to this atmosphere of heightened risk? They have two options: hire more people, which is difficult because of the burgeoning skills gap in the talent market, or rely on AI, automation, and analytics to detect and respond to threats in real time. Due to recent shifts in technology, the latter option—cyber AI—is becoming increasingly effective.

The intersection of AI and cybersecurity has been talked about for nearly a decade. Until now, those conversations revolved around buzzwords and rule-based products. Thanks to advances in compute power and storage capacity, we now see cybersecurity vendors starting to truly incorporate machine learning and AI into their products. Today, large enterprises can rely on such vendors to advance threat intelligence.

Premier cybersecurity vendors have deployments across many enterprises, which serve as sensors for picking up data. By applying AI to the anonymized data from each customer, vendors can use the threat data from one organization to look for signs of similar breaches elsewhere. The network effects can be exponential: The bigger and more diverse the dataset, the more these vendors' detection improves, and the greater their protection. For this reason, medium and large enterprises alike could benefit from working with managed service providers. Or, alternately, they can have their data science and cybersecurity teams work together to train AI models in their own cybersecurity warehouses.

Today's computing power allows the development of sophisticated user and entity behavior analytics (UEBA) that detect signatures of bad actors or deviations from normal behavior. UEBA might flag a user who is detected downloading terabytes of data on a Saturday morning—certainly not a habit. By connecting these profiles and patterns, threats can be identified in a far more refined manner.

While these signals always existed, it was previously impractical to analyze them and draw meaningful patterns. Now, these AI-flagged threats can be fed into security orchestration, automation, and response (SOAR) platforms, which can shut down access or take any other immediate actions.

The history of cybersecurity, and really any type of security, is an age-old game of cat and mouse. Just as we develop AI tools to protect ourselves, antagonists are

developing AI to further complicate their attacks. Nation-states are already entering this territory, and we may see more from private cybercrime actors in the next 18 to 24 months. If organizations don't want to be a victim, they'll want to act now to future-proof their users, systems, and data by seeking out opportunities for AI support. When the nature of cyberattacks inevitably transforms again, they can be ready.

MY TAKE

Adam Nucci

Deputy director of strategic operations, US Army

The US Army is in the midst of a modernization journey that requires us to adopt a data-driven mindset and embrace digital transformation.

The objective is to evolve not only weapons systems and platforms but also processes, workforce, and culture.

As we modernize, our already-complex technological environment is becoming even more dynamic, and we're challenged from all sides by a broad range of sophisticated adversaries. To meet our ambitious modernization goals, it's critical that we elevate our security posture. Fortunately, the future is now: The tools needed to do this effectively are here today. But a focused effort is required not only to use them for security but also to alter the ways in which capabilities, networks, and talent are delivered. It is vitally important to build in adaptive security. Massive amounts of data are being generated by technology systems and sensors. Advanced analytics techniques

and platforms can be used to rapidly analyze and act upon this data. And the broad adoption of cloud computing enables real-time data-sharing as well as full-spectrum data and network management, control, and visibility.

We have the building blocks at hand. The powerful combination of data, analytics, and cloud computing serves as the foundation of zero trust–based security approaches centered on data rather than networks—especially the migration from network-based identity and credential management to data- and device-centric identity access management and least-privilege access principles. This sets the stage for the use of cyber AI at scale.

With machine learning, deep learning, and other AI techniques, organizations can understand the cybersecurity environment across multiple hardware and software platforms; learn where data is stored, how it behaves, and who interacts with it; and build attacker profiles and propagate them across the network environment. AI and predictive analytics can also help us better understand some of the human-related aspects of cybersecurity. Across the operational environment and broader society, the information dimension is woven inextricably into the fabric of just about everything; advanced machine learning and AI have the potential to help us understand how the information sphere impacts users, how we make decisions, and how adversaries behave.

Today's AI is not general-purpose; it's primarily fit-for-purpose solutions built for sometimes narrow but mostly specific use cases. But cybersecurity isn't a narrow problem that can be solved by technology alone; it's primarily a *people* problem. Our adversaries are diverse and creative. What makes them tick? To advance cyber AI, we need to bring that same variety and imagination to the cyber workforce. We need to cross-pollinate the traditional STEM-educated, linear-thinking cyber workforce with application mavericks and polymorphic thinkers who can draw inferences based on not-so-obvious connections. Not only does this add a human dimension to model building and training, it also creates a cybersecurity force multiplier.

Driven by data, analytics, and the cloud, an AI-driven cyber strategy enables organizations to predict, detect, and counter intrusions in an automated fashion. There are emerging challenges and opportunities in mobile and low-bandwidth environments, but the technology foundation is in place.

To further enable cyber AI, we also need stronger collaboration between the public and private sectors. Cybersecurity *is* national security. We as

a society need to elevate cybersecurity from a bolt-on afterthought to the embedded backbone of all commercial and governmental systems. But the public sector can't succeed alone. With strong public-private partnerships and cross-pollination among industry, academia, and international partners, we can build an unshakeable cybersecurity foundation based on sensor-embedded systems, data, and AI-driven predictive analytics.

EXECUTIVE PERSPECTIVES

STRATEGY

Cyber risk is a more important strategic concern than ever. With the amount of data organizations collect and the breadth of their partnerships and workforce, protection is growing more complicated. Cyber AI is now a leading practice for guarding against the volume and sophistication of recent cyberattacks. CEOs should be asking questions of their CRO, CISO, CIO, and others to understand the current security posture, and whether it needs to be upgraded. By positioning AI as a security and strategy priority, leaders can help their organizations align on the importance of strengthening defenses and managing risk.

FINANCE

As the prevalence and financial impact of cyberattacks increase, CFOs are taking an expanded role in overseeing risk management. They should use their unique role in C-suite leadership to advocate for a fully funded enterprisewide adoption of AI-enhanced cyber defense. They can work with their cybersecurity teams to understand the investment required, timeline, risks, and benefits of cyber AI, and then present that information to the board as a key priority.

RISK

Bad actors have been leveraging AI for years to conduct cyberattacks. CROs should prepare their organizations for the new normal of fighting those attacks with AI defense and intelligent security operations. Organizations should find internal support to build these new capabilities or evaluate outsourcing cyber protection to augment their security teams. Of course, AI defenses have their own vulnerabilities, and the threat landscape will continue to evolve. Acting now to begin improving defenses gradually—rather than reacting when it's too late—can help organizations protect customers and their data.

ARE YOU READY?

KEY QUESTIONS

1 How has your enterprise attack surface expanded due to an increase in remote workers, network-connected devices, and third-party risk, and what steps are you taking to protect it?

2 How are you currently using AI tools to detect, contain, and respond to cyberthreats? In which areas can the use of AI be expanded to create a more proactive security posture?

3 Do you have the skill sets and organizational structure needed to meet your cybersecurity objectives today? In two years? How do you plan to acquire these skills?

LEARN MORE

Zero trust: Never trust, always verify

See how a zero-trust cybersecurity posture provides the opportunity to create a more robust and resilient security.

2021 Future of cyber survey

Gain insight from nearly 600 global C-level executives who have visibility into the cybersecurity functions of their organizations.

State of AI in the enterprise, 4th edition

Discover what today's AI-fueled organizations are doing differently to drive success.

AUTHORS

Our insights can help you take advantage of emerging trends. If you're looking for fresh ideas to address your challenges, let's talk.

Curt Aubley
Cyber & Strategic Risk groups managing director
Deloitte & Touche LLP
caubley@deloitte.com

Ed Bowen
Advisory AI CoE leader
Deloitte & Touche LLP
edbowen@deloitte.com

Wendy Frank
Cyber 5G leader
Deloitte & Touche LLP
wfrank@deloitte.com

Deb Golden
US Cyber & Strategic Risk leader
Deloitte & Touche LLP
debgolden@deloitte.com

Mike Morris
Cyber & Strategic Risk managing director
Deloitte & Touche LLP
micmorris@deloitte.com

Kieran Norton
Cyber & Strategic Risk infrastructure security solution leader
Deloitte & Touche LLP
kinorton@deloitte.com

SENIOR CONTRIBUTORS

Wil Rockall
Partner,
Deloitte LLP

Jan Vanhaecht
Partner,
Deloitte Belgium CVBA

Sam Holmes
Senior manager,
Deloitte LLP

Ryan Lindeman
Senior manager,
Deloitte & Touche LLP

PaPa Yin Minn
Specialist master,
Deloitte Tohmatsu Cyber LLC

ENDNOTES

1. Steve Morgan, "Cybercrime to cost the world $10.5 trillion annually by 2025," Cybersecurity Ventures, November 13, 2020.
2. IBM, *Cost of a data breach report 2021*, accessed November 17, 2021.
3. Ibid.
4. *CNBC*, "Cybercrime could cost $10.5 trillion dollars by 2025, according to Cybersecurity Ventures," March 9, 2021.
5. *PR Newswire*, "Artificial intelligence-based cybersecurity market grows by $19 billion during 2021-2025," June 21, 2021.
6. NCCI, "Remote work before, during, and after the pandemic: Quarterly economics briefing—Q4 2020," January 25, 2021.
7. Jasper Jolly, "Huge rise in hacking attacks on home workers during lockdown," *Guardian*, May 24, 2020.
8. Fleming Shi, "Surge in security concerns due to remote working during COVID-19 crisis," Barracuda, May 6, 2020.
9. Cisco, *Cisco annual internet report (2018–2023) white paper*, accessed November 17, 2021.
10. Gartner, "API security: What you need to do to protect your APIs," accessed November 17, 2021.
11. David Flower, "5G and the new age of fraud," *Forbes*, December 30, 2020.
12. GSMA, *The mobile economy*, accessed November 17, 2021.
13. Steve Rogerson, "Cellular IoT connections grew 12% in 2020, says Berg," IoT M2M Council, August 4, 2021.
14. (ISC)², "(ISC)² study reveals the cybersecurity workforce has grown to 3.5 million professionals globally," accessed November 17, 2021.
15. Wendy Frank (Cyber 5G leader at Deloitte & Touche LLP), interview, October 1, 2021.
16. Palo Alto Networks, *The state of incident response 2017*, accessed November 17, 2021.
17. Critical Start, *The impact of security alert overload*, accessed November 17, 2021.
18. Matthew Hutson, "Artificial intelligence just made guessing your password a whole lot easier," *Science*, September 15, 2017.
19. Lily Hay Newman, "AI wrote better phishing emails than humans in a recent test," *Wired*, July 2021.
20. William Dixon and Nicole Eagan, "3 ways AI will change the nature of cyber attacks," World Economic Forum, June 19, 2019.
21. Ibid.
22. Matthew Hutson, "Artificial intelligence just made guessing your password a whole lot easier."
23. Tony Pepper, "Why contextual machine learning is the fix that zero-trust email security needs," Help Net Security, February 16, 2021.
24. Al Dillon (cofounder and CEO, Sapper Labs Cyber Solutions), phone interview with authors, October 19, 2021.

The tech stack goes physical

ACHIEVE SYSTEM RESILIENCY

Mission critical physical systems cannot fail.

RECONSIDER GOVERNANCE

Smart devices bring new governance challenges.

REFRESH TECH EXPERTISE

Smart devices require new and different IT skill sets to manage, monitor, and maintain.

TREND 6

The tech stack goes physical

CIOs increasingly need to manage physical technology stacks

With the wide availability of advanced processors and sensors, industrial robots, and machine learning, any device can be smart, connected, and capable of capturing data and establishing feedback loops to improve products and services and generate new revenue streams. As the range of physical devices and capabilities explodes, chief information officers' (CIOs') remits are being expanded again, beyond the digital, to broadly encompass these new physical assets.

For decades, IT organizations have focused on managing technologies, tools, applications, frameworks, data ecosystems, and other elements of a primarily digital tech stack. Historically, the physical tech stack has been far less dynamic, consisting primarily of employee access points and data center infrastructure.

As it moves onto the shop floor and into operations, technology is evolving from business enabler to value driver, becoming the linchpin of the enterprise. Today, the digital capabilities of security, automation, data-driven analytics and decision-making, and artificial intelligence (AI) and machine learning are needed to manage smart devices across the enterprise. Consider, for example, that by 2025, 30% of new industrial control systems will include analytics and AI-edge inference capabilities, up from less than 5% in 2021;[1] or that connected passenger vehicles are expected to generate 10 exabytes of data per month by 2025.[2]

From milling machines in manufacturing plants, connected heart monitors in hospitals, and inspection drones for infrastructure, to robot cookers in restaurants, smart sensors in office buildings, and new "phygital" consumer products, a new generation of physical assets is being embedded with advanced digital technologies to enable business-critical functions. IT organizations are increasingly on the hook to manage, monitor, measure, and secure these assets. CIOs must wisely choose technologies based on application, device, and security requirements and consider how they will onboard, manage, and maintain devices and networking technologies that now require the highest levels of uptime and redundancy. They must

also rethink device governance and oversight, and reconsider how the technology workforce is organized, defined, managed, and trained.

Raising the stakes for uptime, redundancy, and security

Many of the devices in the new physical tech stack provide customer-facing, business-critical applications and services. They often generate and use a high volume of data and video, which needs to be rapidly moved and analyzed to facilitate real-time, critical decision-making.

Unlike earlier generations of physical devices, an outage could be much more than an inconvenience—it could be business-threatening (a restaurant ordering system goes down, leading hungry customers to find lunch elsewhere) or even life-threatening (an implanted heart monitoring device goes offline, causing critical patient data to be disregarded).

Resiliency is critical; the highest levels of system uptime, reliability, and security likely will be required. As the impact of the physical tech stack on business operations continues to grow, organizations likely will need to consider how to manage and maintain a new generation of connected devices, wireless networks, and edge computing to ensure the highest standards of business continuity. Some of the most significant areas are listed below.

Device and data management

To optimize device and system performance, IT organizations may need to deploy and manage—often remotely—an ecosystem of connected devices, applications, and networks from multiple vendors. New platforms, tools, and approaches may be needed to monitor device health, detect and troubleshoot problems, and manage software and firmware updates. Teams likely will need to build multiple layers of redundancy into devices.

Automation is critical for eliminating repetitive, manual device management tasks, especially for large deployments. Automated device management tools can help organizations scale device registration, configuration, provisioning, maintenance, remote and over-the-air firmware and software updates, and monitoring.

To improve performance or develop new products and services, organizations likely will need to manage the massive amounts of data generated by these devices. IT will need to consider data capture frequency, processing time, accuracy, and formats, among other issues. Data storage will be critical, and in the case of remote environments, distributed storage and edge computing may be preferable.

Wireless networking

To determine the most efficient and resilient solutions for connecting these devices to the network, IT departments need to evaluate attributes such as power consumption, signal strength and range, interference related to physical objects and structures or weather and environmental factors, electrical or radio frequency interference, cost, number of devices being connected, frequency-sharing, security, resiliency, and need for a constant internet connection, among others.

Many smart devices operate on the customer premises or other remote, real-world environments, and are enabled by advanced wireless connectivity, including 5G, Wi-Fi 6, Bluetooth Low Energy, mesh networks, and satellite. Such technologies provide high throughput, low latency, and high capacity, enabling higher data rates.

According to a Deloitte survey conducted in 2020, the pandemic accelerated enterprise investments in newer wireless networking technologies—especially 5G and Wi-Fi 6, regarded by survey participants as the two most critical wireless technologies for business initiatives.[3] Both technologies have performance and operational improvements over their predecessors that promise to support devices, users, and traffic at scale, enable immersive experiences, and help organizations be more resilient. Both enable new applications based on the Internet of Things (IoT) and other emerging technologies that leverage low latency to collect and share mountains of real-time data at the edge.

Wireless networking technologies are complementary; several may coexist or be combined to support multiple use cases. In the same way that many organizations diversify energy technology and generation sources to guarantee continuous operation even in a devastating storm, they may need to similarly diversify the use of wireless networking technologies to ensure redundancy.

Edge computing

Despite the performance upgrades of 5G and Wi-Fi 6, the cloud cannot ensure acceptable response times and data transfer rates needed for autonomous vehicles, smart factories, augmented and virtual reality, and other applications that require network latencies of tens of milliseconds or even sub-milliseconds. When device-generated decentralized data needs to be processed in real time, a distributed compute solution such as edge computing for processing is more efficient than the public cloud or a data center.

With compute power closer to data sources, edge computing architectures provide the latency and bandwidth needed to manage, process, and extract value from a titanic

volume of data in real time. But don't call it a comeback—edge computing has been here for years. Seventy-two percent of IT leaders already use edge computing, according to a recent survey;[4] and Gartner predicts that by 2025, more than 50% of enterprise-managed data will be created and processed outside the data center or cloud.[5] Growth is imminent: One edge computing industry organization projects that between 2019 and 2028, cumulative expenditures on edge computing devices and equipment will be up to $800 billion, with the most notable increases occurring in manufacturing and health care.[6]

Seventy-two percent of IT leaders already use edge computing.

Given the business-critical nature of edge computing sites—which are often unstaffed—redundant power, cooling, and network connectivity are critical, as are physical security and remote monitoring and management.

New approaches to governance and oversight

Governance and oversight strategies and policies may need to evolve to meet the needs of a new generation of connected devices. Regulations and standards related to physical devices and network usage may be unfamiliar and challenging to IT organizations and remain in flux for many years. Consider that it took the better part of two decades before US courts replaced a patchwork of state tax laws with a definitive ruling on e-commerce sales tax.

Here are some key governance considerations related to devices, data, and security.

Devices

Operating certain physical assets may be regulated by federal, state, or local restrictions. For example, US organizations using outdoor drones must register them and gain airspace authorization from the US Federal Aviation Administration; certain types of drones must carry an onboard wireless identification system.[7]

Similarly, laws governing the use of autonomous vehicles vary from country to country and even from state to state. No federal rules exist in the United States, only a hodgepodge of state laws governing the use of commercial vehicles, operator licensing, in-vehicle operator requirements, speed limits, and liability insurance, among others.[8]

Liability could become increasingly complex. For instance, if a computer-actuated smart device makes a mistake and harms a human

or damages property, who is responsible, the vendor or the operator? What are the consequences of an AI-driven decision that causes harm? Insurance for certain devices may be advised or required.

Another issue is ownership and maintenance of remotely managed devices, including responsibility for security, upkeep, and repair, and the impact of this on service levels. Asset decommission should be included in device life cycle management, with plans in place for replacing single or multiple assets, revoking certificates, archiving data, and deleting confidential information.

Device procurement may present new challenges, such as distinguishing between enterprise-grade and mass-market smart devices that do not meet rigorous enterprise specifications. As the ecosystem of traditional IT vendors expands to include operational technology and industrial IoT suppliers, the nature and culture of procurement will change.

Data

CIOs and chief data officers may have to consider ownership of the data and metadata produced by network-connected devices. For example, who is legally allowed to copy, distribute, or create derivative works based on this data and metadata? Who controls it?

As with traditional connected devices and applications, ensuring data privacy remains a top priority. Collecting and securing end-user data according to the General Data Protection Regulation (GDPR), International Organization for Standardization, National Institute of Standards and Technology Cybersecurity Framework, Health Insurance Portability and Accountability Act, Federal Information Security Management Act, and other industry and geographical regulations and guidelines is table stakes. Organizations must also consider that sensor- and camera-based devices typically collect and share data continuously, sometimes without explicit end-user knowledge or permission. For example, a still or video image that can be used to identify a living person constitutes personal data under GDPR and should be collected and protected accordingly.[9]

Security

Securing these physical assets can be challenging because they're often developed with proprietary operating systems and communications protocols, weak built-in security, and limited device memory and computing power.[10] A recent analysis of more than a million enterprise and health care IoT devices found that 98% of all device traffic is unencrypted and 57% of devices are vulnerable to medium- or high-severity attacks.[11] Business-critical assets

located outside of the enterprise firewall pose new security threats, especially when embedded with data, machine learning algorithms, and other intellectual property.

Like traditional networked equipment, these connected devices must be able to securely communicate with the cloud and other network devices and endpoints, encrypt data, and be network-authenticated. Most major cloud providers include security functions in their device management platforms, or IT can develop and install custom security protections to ensure that all devices are actively monitored and protected.

The device procurement process should include security and third-party data access considerations. Choose vendors wisely; on some IoT devices, security researchers discovered hidden backdoors that could be used to send information back to the manufacturer.[12]

Product engineering services: R&D for smart, connected products

As the tech stack goes physical, product R&D is necessarily evolving from an emphasis on standalone products (speakers, thermostats, and cars) to smart, connected platforms with flexible consumption models and data that needs to be moved and analyzed in real time (speakers that stream music from cloud-based services, thermostats with automatic adjustment settings and app-based controls, and cars with remote diagnostics, service, and upgrades). Such products are complex and often require the concurrent transformation of business models, IT systems and capabilities, and business processes.

Product engineering services, or PES, is an integrated process for creating these complex products, from concept design to software and hardware development to manufacturing. PES can include, for example, developing and integrating hardware components such as a CPU or a GPU; the operating system, device drivers, and firmware and other embedded software used to operate the hardware; and application software that provides features, functionality, and user interface. Another critical PES activity is connecting smart products to enterprise IT systems or cloud-based platforms for tracking and billing consumption, monitoring performance, and collecting analytics. Finally, PES helps product teams tap into the rich ecosystem of third-party vendors and partners that may be needed to create or monitor sensors and other hardware and develop applications for use in app stores, e-commerce sites, and other distribution channels.

New expertise and skill sets required

As physical assets evolve to be business-critical and are located outside of traditional enterprise boundaries, new skill sets will likely be needed to manage, maintain, and monitor them.

For example, IT organizations may need to build important technical, security, and resiliency requirements into devices and networks: They could need electrical engineers to develop sensors; systems engineers who can program low-power electronics to perform tasks such as signal processing, sensor conditioning, and communication protocols; or engineers who understand radio frequency spectrum management to help with wireless network planning, analysis, design, and optimization. Industrial facilities may need to integrate connected sensor-based devices and instruments with legacy manufacturing systems, industrial applications, and command, control, and monitoring systems.

Data scientists and AI and machine learning engineers, including those specializing in video and image analytics, will be needed to help organizations manage the data, uncover insights, automate decision-making, and train algorithms and models. Other specialists will be needed to address issues surrounding data capture, storage, exchange, privacy and protection, and ownership.

In addition to the usual management and soft skills, IT project managers likely will need to be more knowledgeable about device security, operational and industrial processes, change management, and end-user training.

CIOs will need to consider whether to outsource or build highly skilled internal teams from the ground up. To reskill existing business and technology talent, organizations can consider outsourced or internal competency centers and training academies.

The way forward

The expanded physical tech stack has the potential to dramatically change how companies create and deliver value. Their business models may evolve because of the capabilities to drive revenue from industrial insights and human-machine interactions. For example, a company might sell monitoring and maintenance of devices as a service as an add-on to device deployment; develop a shared asset model in which customers sell extra capacity back into the market; leverage sensors to develop a program for automatic reordering of consumables such as printer

cartridges; expand from a reseller model to direct-to-consumer model; or monetize their device data, to name only a few.

Business leaders likely will need to gauge the impact of the emerging physical tech stack on various business areas. Business cases need to be carefully considered, especially for large numbers of inexpensive devices. In some cases, the cost of device management and maintenance could exceed the potential return, even if cheap devices are simply replaced upon failure.

These sensor-embedded, data-driven assets are often business-critical; IT departments likely will need to ensure they have the highest levels of resiliency, upgrade wireless networking and edge computing capabilities to meet stringent latency and throughput requirements, and become familiar with emerging asset management and governance requirements that may be applicable to new devices. Finally, CIOs may need to reconsider how the technology workforce is organized, defined, managed, and trained. To find the required technology skills, CIOs will have to consider whether to reskill and retrain existing talent, hire new technology workers, or outsource the needed skills.

LESSONS FROM THE FRONT LINES

The sky's the limit: How IoT can make better sense of data in aviation

Known for its dedication to customer service, Southwest has long collected customer transaction data on ticket purchasing, check-in, and boarding to continually fine-tune the passenger experience and improve operational processes. But as the airline pieced together transaction data, it discovered a data gap: Because many interactions occurred outside of transactional systems, they weren't being logged and couldn't be measured.

To fill this hole, Southwest began experimenting with the Internet of Things (IoT). The airline's earliest foray was part of a quest to improve aircraft turn time—the time needed to deplane passengers, prepare the plane for departure, and load passengers for the next flight. Starting seven years ago, Southwest piloted an initiative to use video cameras and computer vision on the jetway to speed airplane load times while maintaining customer privacy. Since then, the airline has continued to test IoT to improve passenger journeys; asset utilization and fleet management; and operations and maintenance. In the realm of passenger journey, Southwest tested the use of Bluetooth and Wi-Fi beacons to see where customers congregate in airports in order to estimate security wait times. When a customer opted into the service during testing through the Southwest mobile app, the system would ping the user's phone as they moved throughout an airport.

This highlights the ways in which advanced machine learning is being paired with physical infrastructure, fueling the rollout of previously impractical applications. However, in addition to enabling new use cases, the trend aids technology teams in managing a growing physical infrastructure, which demands new skills along with greater uptime and reliability, says Justin Bundick, director of data science and automation at Southwest.[13]

One of the most important issues to address when building IoT infrastructure is managing the complexity of the "many-to-many relationship," says Bundick. Traditional IT infrastructure needs to complement a variety of physical devices and algorithms in order to support a range of use cases, and that holds for IoT infrastructure as well: "You have to make sure it's not monolithic, that it's scalable and that you're partnering with the right IT infrastructure providers to have something that's resilient."[14]

Another important learning for the team at Southwest has been around testing. While developers can fix digital systems from anywhere, it's more complicated to repair physical infrastructure, particularly in high-security environments such as airports. For this reason, anything Southwest puts into production needs to be solid and reliable, says Kevin Kleist, emerging trends advisor at Southwest: "Testing in a real-world environment provides us with the opportunity to learn more about the viability of a particular solution while also obtaining key insights and understanding the risks."[15]

To get IoT right takes a broad mix of talent and skill sets. For example, facility engineers are needed to understand installation, and cybersecurity experts are needed to mitigate physical devices' unique vulnerabilities. Plus, it's important to remember that the "data created by IoT devices is just a big pile of bits and bytes unless you have a data scientist to analyze it," as Bundick notes.

Angela Marano, managing director of business transformation at Southwest, says it's been important for her team to assess areas where it can add unique value versus where it makes sense to partner with a vendor. When her team is asked to solve a new problem, she evaluates what skills, data, or capabilities are available that would enable her team to create something better than commercial offerings. Sometimes the answer is yes, while other times it's more advantageous to use existing best-in-class solutions.

"Today we have a healthy balance of adventure and pragmatism. In other words, what is this really doing for the business?" Marano says. "We have to make sure we truly understand where we have real competitive advantage."[16]

Drones revolutionize electrical infrastructure inspections

Southern California Edison (SCE) has been a pioneer in the use of drones to inspect its electrical infrastructure. In a service area of approximately 50,000 square miles, the utility uses drones to help verify the integrity of poles, lines, towers, transformers, and other distribution and transmission structures. Safer and more lightweight, maneuverable, and cost-efficient than helicopters, drones help SCE crews speed inspections and collect more accurate data, particularly in areas considered at high risk for wildfires.

In 2021, 75% of the approximately 200,000 structures in wildfire-risk areas were inspected by drones, up from 25% in the previous year—an increase driven by drones' ability to enable more thorough, faster, and more

accurate inspections. "Compared to helicopters, drones can get closer to the structure and get shots from many angles and viewpoints," says Vibhu Kaushik, SCE's director of inspections.[17] "We get tighter shots, more shots, and better shots that improve our visibility of potential equipment problems, vegetation hazards, and other ignition risks."

"Plus, drones allow us to rapidly scale the number of structures we inspect," he continues. "They're more cost-efficient than helicopters, and it's easier to hire drone pilots or train inspectors to fly drones."

The rapid expansion of its drone inspection program presented SCE with a variety of growth-related challenges and opportunities. For example, initially inspectors stored images on their laptops. As the number of these high-resolution images rapidly escalated, laptop storage became infeasible. SCE migrated to a cloud platform and now images captured in the field by two-person drone crews are transferred directly to the cloud to be viewed and evaluated by in-office inspectors.

Kaushik's team is currently testing a modified process in which inspectors themselves are trained to fly drones. As inspector-led drone teams conduct inspections, images are stored in the cloud and evaluated in the field on tablets. Drone flights can be preprogrammed using GPS coordinates, enabling inspectors to focus on evaluating images.

The sheer volume of images collected poses additional challenges. SCE's service area includes approximately 1.4 million distribution poles and 140,000 transmission structures, and inspections require 10 to 12 images of each structure; inspecting larger transmission towers requires capturing between 400 and 600 images. "As we look to the future, it's not sustainable for every image to be reviewed by a human inspector," says Kaushik.

To eliminate the image bottleneck, SCE is developing and training AI models to identify defects in utility poles, insulators, and transformers, among other structures, feeding the models with thousands of photos so they can automatically pinpoint structures needing remediation. The models will take the first pass at evaluating inspection images, notifying human inspectors when anomalies are detected. "Instead of inspecting millions of images, human inspectors can prioritize those identified as having a defect or a chance of a defect," explains Kaushik. "That will enable us to more quickly find and remediate those structures."

Kaushik reports that as SCE's AI models mature, they're delivering good true positive and true negative success rates.

Customer awareness and acceptance were other challenges to drone inspections. SCE developed a comprehensive community

outreach program and worked with local law enforcement agencies to educate and inform community members. "We also learned how important our brand is. Acceptance was lower when the link to SCE was not obvious," says Kaushik. "But when we leverage the SCE brand and work proactively to build community awareness, people are generally positive and receptive."

Moving forward, SCE is expanding the use of drones to inspect dams and other generation structures, and to assist maintenance and repair crews with damage surveys and repair inspections. "SCE is committed to using drones to improve the resilience, safety, and efficiency of the grid," Kaushik says. "Technologies such as drones and smart sensors are helping us develop the energy grid of the future—one that's decarbonized, distributed, decentralized, and automated."

Sheba Medical Center sets the standard for smart hospitals

Sheba Medical Center of Israel has ranked among the world's best hospitals for years, due in part to its use of smart devices and other digital technologies.[18] The Ramat Gan–based medical center, which treats nearly 2 million patients a year, also hosts 75 research laboratories and the ARC (Accelerate, Redesign, Collaborate) innovation program for Sheba's clinicians and health care startups.

To improve patient care, Sheba is leading innovations in telemedicine powered by sensors and cameras, AI for diagnosing CT scans, and many more areas of health care.[19] For example, while many smart hospitals deal with alert fatigue—doctors being overwhelmed by the abundance of electronic nudges and notifications from medical equipment—Sheba has developed methods for integrating technology to improve quality, safety, and efficiency without distracting medical staff. Says Dr. Eyal Zimlichman, chief innovation officer at Sheba, "A smart hospital should use AI and smart devices to help doctors be more effective, not remove their autonomy."[20]

Sheba is providing AI-based decision support in the intensive care unit (ICU) to help doctors attend to complicated and critical patient issues in a data-intensive environment with a high level of uncertainty. Patient sensors in the ICU, such as arterial blood pressure sensors, generate a high volume of data that is analyzed by Sheba's AI platform to provide doctors with critical alerts and suggestions for care. Given the high-risk setting, many mistakes can be made without the right insights. "Every decision in an ICU can have a huge impact on patient health and hospital

efficiency, so we focus our decision support on improving ICU risk," says Zimlichman.

The hospital also leverages AI and data from hospital devices to tackle operational issues. In any hospital, managers need to direct the flow of activity and patients, but decisions are often not made based on data. Sheba's team, together with several startups, is building a control tower application that uses real-time data from patient beds to maximize the efficiency of operating bed assignments and patient allocation. The team is also working on continuous care applications, leveraging wearable tech such as smart watches, to monitor patients with chronic diseases. "By building a digital environment to match patient needs, we can complement the traditional methods and reduce hospitalizations," says Zimlichman.

At present, the ARC team is working on arming doctors with AI-enabled video analytics during surgery so surgeons know whether their incision is being made in the right place or if bleeding has crossed a safe threshold. As the technology improves, eventually surgical robots will independently carry out operations, starting with (relatively) simple tasks such as opening a patient's abdomen. In 10 to 20 years, Zimlichman believes robots will be able to take on the most complicated surgical procedures and even remote surgery. "In the future, robots will complete 95% of the surgery, like autopilot on airplanes. Surgeons will simply monitor and carry out the other 5%," says Zimlichman.

Hospitals are currently a major driver of health care costs, but Sheba has proven they can be more sophisticated, efficient, and safe with technological improvements. According to Zimlichman, as further progress occurs, hospitals may play a smaller role and be physically smaller because technology will enable doctors to perform most patient care outside the hospital. Says Zimlichman, "COVID has accelerated the change in hospitals, and we will see the new reality in our lifetimes."

MY TAKE

Brad Chedister

Chief technology and innovation officer, DEFENSEWERX

Increasingly, organizations are relying on connected devices to provide new and better services and products.

Using unmanned aerial systems (UAS), they're making deliveries, inspecting railroads, and conducting reconnaissance missions. From factories and fast-food restaurants to hospitals and defense agencies, they're leveraging robotic equipment to automate processes and improve efficiency and delivery. But in the age of smart, connected, and automated organizations, we should never forget that humans are more important than hardware.

My organization's technology development and innovation initiatives are designed to help defense agencies solve difficult problems. We operate several innovation hubs across the United States to cultivate innovation ecosystems that help us develop solutions to protect our nation. In my work, I've observed that as organizations become more data- and device-driven, challenges often arise where people and technology intersect.

For example, when people with legacy system and process expertise have to migrate to new technologies and new ways of working, the importance of workforce development goes without saying. But sometimes a cultural shift is also needed. When developing an innovation initiative, some people might start out with the sentiment "We can't do that because ..." For example, we can't do that because it's not interoperable with legacy systems, or because it will take too long to deploy and implement.

I encourage teams to shift their thought process from "We can't do that because ..." to "What if we could?" For example, what if we *could* develop an automated CRM tool that can sift through an ecosystem of more than 85,000 innovations to discover novel tools to solve warfighter issues? Without the sentiment "What if we could?" and the culture that accompanies it, smart automated tools and systems will probably never move past the starting point.

Such a cultural shift can help organizations find and hire the talent with the technical skills needed to be innovators. Organizations have to do more than simply remain relevant; they have to attract the workforce of the future—talent with the technology chops to work with UAS and other unmanned vehicles, robotics, sensors, AI and machine learning, data analytics, and other key technologies.

Another challenge related to people and technology, particularly with regard to automation and robotics in private companies, is the idea that technology eliminates people's jobs. In the defense industry, our most important assets are our warfighters—not equipment or technology—and so our focus is on using technology to protect our people.

For example, when we use UAS to scout out unknown territory, we're keeping soldiers out of harm's way. And as it turns out, a UAS with intelligence, surveillance, and reconnaissance software and short-wave infrared imagery capability can "see" 10 times as far as a human—so UAS are also a force multiplier. Similarly, businesses can consider how to leverage smart devices and automation to accomplish dangerous tasks that traditionally have been completed by humans, and they will probably realize some efficiencies or other improvements along the way.

Whether in the private sector or the public sector, some activities are intrinsically human. Tasks requiring trust and warmth require personal interactions and will never be replaced by AI or a robot. But the trend of automating tasks and roboticizing systems is not likely to slow down as long as it continues to help make workplaces safer and more efficient.

EXECUTIVE PERSPECTIVES

STRATEGY

CEOs are increasingly concerned with technology-driven customer experience, which increasingly requires alignment between IT and physical technologies. Physical technologies require different standards for resilience. Case in point: An autonomous vehicle that shuts down or malfunctions can present serious risks to passengers and bystanders. CEOs should validate that their teams have the capacity to meet the standards of new physical tech, particularly in areas where human safety is paramount. They can work with IT leaders to ensure the culture around physical tech prioritizes customer safety, security, as well as convenience.

FINANCE

Given how crucial smart devices are becoming, IT is overseeing ever-more varied devices. CFOs should take the opportunity to review the cost impacts and changes in risk exposure, including potential damage to reputation or shareholder value in the event of failures or security breaches. CFOs can help IT collaborate cross-functionally with risk, compliance, and other functions. Moreover, they may want to review their investments to understand the appropriate budgets for software, hardware, and physical technology.

RISK

Although connected devices and enablers like 5G networks garner a lot of attention, the details of their multifaceted security requirements are still being defined. As physical technology becomes increasingly critical, such as medical devices or factory robots, the stakes of failure rise dramatically. CROs should work with the IT and business to identify potential security concerns and corresponding risk requirements. They can also work with the CEO and CIO to emphasize reliability and create a culture of risk management.

ARE YOU READY?

KEY QUESTIONS

1 How can you harden your technology infrastructure to provide the uptime, redundancy, and security needed to maintain the new generation of connected devices and physical assets?

2 What regulatory or compliance mandates might impact your management of larger numbers of increasingly complex physical assets?

3 What skill sets will be needed to manage, maintain, and secure multiple and diverse connected devices? Do you have access to these skill sets, and if not, how will you acquire them?

LEARN MORE

CXOs and 5G edge networks: Investing today for tomorrow's competitive advantage

See how 5G edge computing technologies can help organizations unleash the next phases of innovation, efficiency, and agility.

Accelerating enterprise innovation and transformation with 5G and Wi-Fi 6

Learn how interest in advanced wireless tech is ramping up in Deloitte's Study of Advanced Wireless Adoption, Global Edition.

Accelerating smart manufacturing

Explore how engaging in smart manufacturing ecosystems can accelerate digital transformation and drive results.

AUTHORS

Our insights can help you take advantage of emerging trends. If you're looking for fresh ideas to address your challenges, let's talk.

Peter Liu

Unmanned Aerial Systems (UAS) and Counter-UAS (CUAS) technologies leader

Deloitte Consulting LLP

peteliu@deloitte.com

Robert Schmid

Internet of Things practice leader

Deloitte Consulting LLP

roschmid@deloitte.com

Sandeep Sharma, PhD

Deputy chief technology officer

Deloitte Consulting LLP

sandeepksharma@deloitte.com

SENIOR CONTRIBUTORS

Brian Greenberg
Principal,
Deloitte Consulting LLP

Britta Mittlefehldt
Director,
Deloitte Consulting GmbH

Tim Paridaens
Partner,
Deloitte Belgium CVBA

Andreas Staffen
Partner,
Deloitte Consulting GmbH

Thierry Cazenave
Senior manager,
Deloitte France

Gabriel Goïc
Senior manager,
Deloitte France

Adam Niedbała
Manager,
Deloitte Poland

Hugo Araujo
Senior consultant,
Deloitte MCS Limited

Nigel Forlemu
Consultant,
Deloitte MCS Limited

ENDNOTES

1. Gartner, *Market guide for edge computing solutions for industrial IoT*, accessed November 17, 2021.
2. Phil Marshall and Philippe Cases, *Enabling the connected vehicle market to thrive*, Topio Networks, accessed November 17, 2021.
3. Jack Fritz et al., *Accelerating enterprise innovation and transformation with 5G and Wi-Fi 6*, Deloitte Insights, March 22, 2021.
4. Intel, *The edge outlook*, accessed November 17, 2021.
5. Thomas Bittman, Bob Gill, Tim Zimmerman, Ted Friedman, Neil MacDonald, Karen Brown, *Predicts 2022: The Distributed Enterprise Drives Computing to the Edge*, Gartner, October 20, 2021.
6. The Linux Foundation, *State of the Edge 2021: A Market and Ecosystem Report for Edge Computing*, 2021.
7. Jaclyn Diaz, "U.S. announces new rules for drones and their operators," *NPR*, December 29, 2020.
8. IIHS, "Autonomous vehicle laws," accessed November 17, 2021.
9. University College London, "Guidance note on the use of images and videos under data protection law," accessed November 17, 2021.
10. Mary Shacklett, "IoT projects demand new skills from IT project managers," TechRepublic, July 14, 2021.
11. Palo Alto Networks, *2020 Unit 42 IoT threat report*, March 10, 2020.
12. Internet of Business, "Security researchers find backdoor in Chinese IoT devices," accessed November 17, 2021.
13. Justin Bundick (director of data science and automation, Southwest), interview, September 8, 2021.
14. Ibid.
15. Kevin Kleist (emerging trends advisor, Southwest), interview, September 8, 2021.
16. Angela Marano (managing director of business transformation, Southwest), interview, September 8, 2021.
17. Vibhu Kaushik (director of inspections, Southern California Edison), phone interview with authors, October 22, 2021.
18. *Newsweek* editors, "The top 10 hospitals in the world," *Newsweek*, March 6, 2020.
19. Sheba Medical Center in Israel, "ARC – The center for digital innovation at Sheba Medical Center," accessed November 20, 2021.
20. Dr. Eyal Zimlichman (chief innovation officer at Sheba Medical Center), phone interview, November 11, 2021.

Field notes from the future

QUANTUM AND THEN SOME

Quantum research goes commercial in the next decade.

EXPONENTIAL INTELLIGENCE: ONCE MORE, WITH FEELING

AI recognizes human emotions.

AMBIENT EXPERIENCE: LIFE BEYOND THE GLASS

Technology for everyone, everywhere.

TREND 7

Field notes from the future

A look at three emerging technologies over the horizon

In the global arena of enterprise technology, optimism rules the roost. We are so enthralled by rapid fire innovation and the opportunity-laden disruption that follows that we have—with considerable justification—developed an abiding faith in technological progress. Today's acorns will become tomorrow's towering oaks, or so the preferred narrative goes.

The challenge with this narrative is that it almost always paints optimistic outcomes with a broad brush. The notion that rapid advances in AI will give rise to exciting new business models in five years is cold comfort to a chief financial officer sweating the next quarterly statement.

The question many leaders, strategists, and technologists rightly ask is, "What can we do right now to prepare for an event whose nature and timing is uncertain?" We offer this humble response: If you wager that something exciting will happen with a number of emerging technologies during the next decade, you will probably win that bet. What exactly will happen? We don't know yet—and neither does anyone else. But in this final chapter of *Tech Trends 2022*, we do offer a framework for thinking strategically about technology possibilities that currently appear small on the horizon.

We focus on three such possibilities that we feel are notable:

- **Quantum technologies,** which are poised to transform computing, sensing, and communications within the next decade
- **Exponential intelligence,** the next generation of AI technologies that promises to understand human emotion and intent
- **Ambient computing**, which will make technology ubiquitous in our work and home environments

We follow our discussion of these possibilities with an essay by Deloitte Consulting LLP's chief futurist Mike Bechtel, in which he looks to the past to find a glimpse of tomorrow.

Read on.

Quantum and then some

Quantum computing, while maturing rapidly, remains the focus of several esoteric debates. One is whether Majorana fermions exist. Admittedly, most people don't have a dog in this fight, but those who do seem ready to rumble. One side believes that Majorana fermion particles—which theoretically contain their own antiparticles—could make remarkably stable quantum qubits. Doubters counter that nobody has been able to find evidence that these particles even exist and, until they do, Majorana's quantum possibilities remain just that: possibilities.[1]

In a way, this debate over theoretical particles encapsulates the state of quantum computing today: Everything is incredibly interesting and promising, but we are still in the early days of quantum exploration. Definitive timelines and research breakthroughs remain works in progress.

Yet there is a widely held belief that we will figure all of this out, and that quantum will loom large in our collective future. Indeed, quantum research is gaining momentum and is expected to migrate from labs to real-world commercial environments within this decade.[2] Technology giants, governments, and early-stage startups are investing billions in a race to achieve quantum breakthroughs.[3]

Promising areas of focus include:

- **Computing.** Quantum computers are special-purpose tools for solving advanced computational problems. They leverage quantum phenomena to process information and make highly specialized calculations. With this in mind, quantum computers probably will not replace classical computers. Rather, they will coexist with their legacy counterparts, and provide advanced computing power as needed for complex computational workloads.[4] To give you a glimpse of quantum computing's potential, in recent demonstrations, quantum machines completed specialized tasks in five minutes that researchers say would have taken classical supercomputers thousands of years to complete.[5]

- **Communication.** Quantum communication is a hardware-based solution that uses principles of quantum mechanics to create theoretically tamper-proof communication networks that can detect interception and eavesdropping. Among several techniques for achieving this level of secure communication is quantum key distribution (QKD), in which parties exchange highly secure encryption keys to transmit data across optical networks. Even though QKD technology is not fully mature, several quantum communication networks have either been deployed or are in development.[6]

- **Sensing.** Thanks to the sensitivity of subatomic particles, quantum sensing devices are more responsive and accurate than conventional sensors. Within the next decade, it is likely that quantum sensors could replace conventional sensors in some applications. Indeed, there are promising use cases in the energy, transportation, and health care sectors, among others. Quantum sensors are available, but at present are somewhat limited. Researchers are working to make them cheaper, lighter, more portable, and more energy-efficient.[7]

Though quantum dynamics is fraught with mind-bending challenges, quantum technologies are advancing. As this maturation progresses, it will be altogether too easy to get caught up in the details of intriguing technologies. What technologist will be able to resist pondering things such as lasers freezing particles and temperatures colder than outer space? Likewise, what business strategist will ignore the investment enthusiasm surrounding quantum technology vendors going public?

Within five years, we will understand much more.

While we may not know with precision the destination of our collective quantum narrative, we have a sense of its direction. And the good news is that within five years, we will understand much more. We may be able to use interesting machines to optimize things such as computing, communication, sensing, and even chemistry. Now is the time for your organization to begin thinking about *that* future. By taking a wait-and-see approach, you could miss critical opportunities to test and experiment with quantum technology while your competitors gain a competitive advantage.

Exponential intelligence: Once more, with feeling

In data-mining folklore, there is an illustrative anecdote involving beer and diapers that many find useful in explaining the traditional state of AI. As the story goes, analysis of supermarket transactions revealed that by placing beer on shelves next to diapers, stores can boost beer sales. What is the correlation between diapers and beer sales, you ask? A data scientist whose name is lost to history theorized that wives ask husbands to pick up diapers on their way home from work. While husbands are picking up the requested supply of diapers, they realize they will need to fortify themselves with beer in order to deal with the tiny individuals who will be wearing said diapers.[8]

Beyond the enduring truth that parenting can be stressful, there is an important underlying lesson here: Machine-driven analysis of sales

transactions can only suggest causation between diapers and beer sales. It takes a human brain to infer and explain the customer emotions and psychology driving those sales. In other words, despite its much-vaunted analytic superpowers, AI has traditionally been unable to distinguish between *meaningful* and *meaningless* statistical connections.

During the next decade, this is likely to change dramatically. In previous *Tech Trends* reports, we examined how a nascent class of AI-powered solutions—referred to as "affective computing" or "emotion AI"—is adding an emotional quotient (EQ) to technology's IQ, at scale.[9] During the next decade, affective computing will continue to morph and grow as innovators train machines, through next-generation deep learning techniques, to both recognize and emulate human traits such as charisma, charm, and emotion. They will, in turn, use "symbolic" and "connectionist" techniques to embed deductive reasoning and logical inference capabilities into AI and artificial neural networks. Soon, these technologies will be able to look at a statistical correlation and, much like the human brain, determine if it makes sense or if it is just a random feature of the supporting data that has no intrinsic meaning. In other words, machines will be able to appreciate the world more as humans do, and less as a context-free collection of zeros and ones.

This represents a shift in our relationship with machine intelligence. Since the AI field emerged in the 1950s, we have valued this curious technology as much for what it cannot as for what it can. It has turbocharged our ability to extract insights from data while never undermining human cognitive and emotional supremacy. However, machines have grown exponentially in power and capability. In our quest for efficiency and insight, we are now designing them to have a level of emotional acuity that is erasing the traditional human-machine cognitive hierarchy.

Pioneering researchers are currently training AI applications to be both versatile and detail-oriented in a very human way. For example, by recognizing common questions in the order in which they are asked, AI-powered bots engage in remarkably humanlike interactions with customers in call centers, restaurants, and banks. The next step might be, for example, creating a senior-care bot with sensors that can distinguish between a lamp falling off a night table and an individual who has fallen and needs assistance. As AI grows in both intuitive and emotional capability over the next decade, bots may begin working as educators, writers, physicians, and even chief information officers.

We believe this process of development, training, and deployment will continue apace for the next decade and beyond. Things that seem uniquely human today will increasingly be expressed as sequences of code. As this happens, business leaders will finally be able

to realize automation's full promise, which will have a transformational impact on value chains, business models, and strategies. A decade may seem like a long time—particularly for decision-makers working feverishly to finalize their next quarterly report. But advances in exponential intelligence will not wait for you. The time to begin automating low-hanging fruit in your organization is now.

And about that scary, dystopian world that science fiction writers have been telling us about for so long? Fear not. The truth is that software has always been neutral, manifesting the explicit orders and tacit biases of its developers.[10] Recently, Deloitte futurists, in collaboration with the World Economic Forum, published *Technology futures: Projecting the possible, navigating what's next*, a vivid examination of future possibilities and approaches for realizing them.[11] On AI's future, the authors write: "As information technology continues to evolve from our *telling* machines what to calculate toward *teaching* machines what to discern, it will be increasingly important for organizations, governments, and regulators to closely monitor the 'curriculum.' How can we develop artificial intelligences that embody our explicitly shared financial, social, and ethical values? We must teach our digital children well, training them to do as we say, not necessarily as we've done."

Ambient experience: Life beyond the glass

Following the advent of command-line interfaces in the 1960s, it seemed only futurists and science fiction writers dared imagine a world in which technology was truly ubiquitous, rather than sequestered behind screens. For most, the understanding that we access computer capabilities and the internet through a glass rectangle became dogma.

Over time, these glass screens became much smaller. They now fit in our pockets and on our wrists. What's more, the number-crunching and networking technologies behind these shrinking screens have become exponentially more powerful and sophisticated, so much so that we're beginning to interface with the cloud directly, without the intermediation of glass. Think about smart speakers. It wouldn't occur to children growing up today in homes with smart technology that there are alternatives to "asking the room" to provide the weather forecast.

During the next decade, ambient computing—a catchall term for a growing field of technologies and techniques that make digital reality available to users anytime and anywhere—will become our standard modality and, in doing so, will usher in an era of life lived beyond the glass.

What does this life look like? Consider the following scenarios:

- **Less friction.** Think back to your first encounter with a desktop computer. Odds are, it came with a hefty paper manual. By contrast, today's mobile devices need only feature a "quick start," itself a digital app. While underlying technologies have gotten more complex, user experiences have gotten simpler. Ambient technologies promise to further lower the friction required to learn and use new tools because—like our children asking the room for a weather forecast—all you have to do is talk. Or gesture. Or glance. You no longer have to journey to a computer lab, or log into a laptop, or even check a mobile device. Indeed, ambient interfaces will lie in wait, patiently inferring what next steps are needed and proactively offering the most efficient way to accomplish them.

  We envision futures in which numerous technologies continuously monitor our environments, working in harmony to automate, or at least streamline, our work and personal lives. Of course, there will be some security and privacy concerns to work through. But we can say with certainty that a more streamlined, frictionless life will become a reality for many of us today, and certainly for our children. Simple wins.

- **More proactive and intuitive.** Imagine a world in which everyone has a personal assistant, one who is exceptionally smart, capable, and attentive. These high-performing assistants are digital, and are backed up by a broad array of sensors, voice recognition, analytic, and exponential intelligence capabilities that work 24/7 to monitor your environment and reduce friction wherever possible. For example, your digital assistant might alert you that it is time to depart for the airport. Rather than having to determine the best way to get there and then using a mobile app to check in, the assistant knows your schedule, preferences, and intent, and will do it all for you. As you pick up your bag and walk out the door of your home, the digital assistant will turn off power to nonessential devices, adjust the air-conditioning to an optimal setting, and activate the home security system.

- **The eyes have it.** Augmenting an individual's physical experience with digital information will be another major dimension of life beyond the glass. We are already seeing how early adopters are using smart glasses and virtual or augmented reality (VR or AR) headsets to overlay digital information onto some workers' fields of vision. Think of this as bringing reality itself online—or, perhaps, painting atoms with bits,

albeit with somewhat primitive brushes. Researchers and entrepreneurs alike are already exploring possibilities for using smart contact lenses and even implanted brain chips to augment our senses and (literally) read our minds. Think about it: Why wouldn't it be natural to look at the sun and see how many hours until sunset? Or look at a bus stop and see how many minutes until the next bus arrives? Curious to be sure, but perhaps preferable to staring at our phones all day.

A more streamlined, frictionless life will become a reality for many of us today, and certainly for our children.

How will our collective journey to an ambient world play out? Incrementally, with future-forward organizations focusing right now on low-hanging fruit and moving steadily to more transformational projects over time. As first step, these pioneers are already working to determine where friction exists right now in their organizations. It may be in interpersonal interactions, cumbersome long-established processes, or even in the way employees use technology. They then explore ways to reduce these pockets of friction with technologies *that are available today*. As an example of this proactive approach in action, consider the airline industry. During the last decade, air carriers have completely transformed the customer experience through digitization, reimagining everything from ticket sales to baggage-handling to seat selection. This effort remains a work in progress, but no one who flew commercially 20 years ago can deny that the path from ticket to tarmac is a simpler customer experience than before. There are similar efforts well underway in retail, hospitality, and finance, among many other sectors.

For customers and workers alike, "easier" goes a long way. The technologies you need to support all of your ambient ambitions may not be available today, but it's clear that they're just over the horizon.

Start living life beyond the glass right now.

MY TAKE

Mike Bechtel

Chief futurist, Deloitte Consulting LLP

As futurists, my team and I spend the lion's share of our time studying the past.

I like to say that we're closet historians. Specifically, we research the history of various technologies and how they've impacted, or failed to impact, the way the world works and lives. With a collective 25 years of innovation study under our belts, we know that predicting a single future is still futile—but projecting plausible futures by applying the patterns of the past can help organizations harness tailwinds, dodge headwinds, and more intentionally shape their next steps.

Looking back to the patent for the first computer in 1840, the basic elements listed are unchanged to this day: interaction (i.e., user interface); information (i.e., data); and computation (i.e., CPU). As outlined in this chapter, if these three elements are thought of as the basic train tracks of IT progress, we can understand what the next stops along the journey will likely be. Interaction beyond mobile devices and virtual reality leads to ambient computing, allowing us to abandon screens and experience the digital world alongside the physical. Information leads to exponential intelligence beyond

AI, a future where machines can learn how to be charming or to compose poetry as well as they calculate a variable. Finally, computation beyond digital bits leads to quantum, where we apply physics to solve problems that are intractable to mathematics.

Along the way to meeting these futures, many upcoming technology innovations that impact enterprise IT will first be manifested in art and leisure, where people take more risks. We've seen ideas such as the "like button" embraced first in consumer circles and then implemented in workplace chat platforms. Similarly, viral videos on social media today could pave the way for new forms of workplace training and onboarding. In other words, tomorrow's IT department might look to us like they're playing games in the metaverse, but, to them, that might be optimal knowledge-sharing.

In the same vein, just as content creation has been democratized, many of the historical burdens around IT have been lifted as well. Problems of database management have been abstracted to the cloud and barriers to creating software have given way to open-source technology and code accelerators. The IT organization of the future will have a much bigger assortment of readymade building blocks available to connect and a much smaller number of applications to justify building in-house. The takeaway: Tomorrow's IT teams will be more conductors than songwriters, putting together the best configurations of existing products rather than inventing new ones for limited use.

The remit of IT leadership must also evolve with the changing remit of IT teams. As technology continues to proliferate and the right set of tools becomes an enabling context as opposed to a key issue, CIOs will increasingly shift their focus to information instead of technology. By spending less time as technicians, they can free up time for higher-order insights about their business and their market. The future CIO stands to become the right hand of the CEO, a consigliere trusted to help steer the organization toward what's new, what's next, and where the organization should invest.

Eyes to the skies; feet firmly on the ground

To bring about this change, IT teams need a constitutional commitment to exploration; otherwise, all their resources will default toward operations. They should firewall and dedicate 5 to 10% of their workforce to pure exploration of what's next, and another 15 to 20% to iterative implementation of the most promising innovation candidates. As Oren Harari said, "The electric light did not come from the continuous improvement of candles." Though the cost may seem prohibitive, the rewards of creating that next lightbulb can be *exponential*. Organizations that manage this balance—both optimizing what's now and enabling what's next—can steer toward their preferred tomorrow.

AUTHORS

Our insights can help you take advantage of emerging trends. If you're looking for fresh ideas to address your challenges, let's talk.

Mike Bechtel

Chief futurist

Deloitte Consulting LLP

mibechtel@deloitte.com

Scott Buchholz

Government & Public Services chief technology officer

Deloitte Consulting LLP

sbuchholz@deloitte.com

SENIOR CONTRIBUTORS

Doug McWhirter
Senior manager,
Deloitte Consulting LLP

Caroline Brown
Manager,
Deloitte Consulting LLP

Amy Golem
Manager,
Deloitte Consulting LLP

Raquel Buscaino
Senior consultant,
Deloitte Consulting LLP

Nelson Launer
Senior consultant,
Deloitte Consulting LLP

Abhijith Ravinutala
Senior consultant,
Deloitte Consulting LLP

Lucas Erb
Consultant,
Deloitte Consulting LLP

ENDNOTES

1. Sergey Frolov, *Quantim computing's reproducibility crisis: Majorana fermions*, *Nature*, April 12, 2021.
2. Scott Bucholz, Deborah Golden, and Caroline Brown, *A business leader's guide to quantum technology*, Deloitte Insights, April 15, 2021.
3. Daphne Leprince-Ringuet, "The global quantum computing race has begun. What will it take to win it?," *ZDNet*, February 9, 2021.
4. Deloitte analysis.
5. Frank Arute et al., "Quantum supremacy using a programmable superconducting processor," *Nature* 574 (2019): pp. 505–10, Daniel Garisto, "Light-based quantum computer exceeds fastest classical supercomputers," *Scientific American*, December 3, 2020.
6. Deloitte analysis.
7. Bucholz, Golden, and Brown, *A business leader's guide to quantum technology*.
8. Gregory Choi, Data mining: Association rules in R (diapers and beer), blog post, Data Science Central, August 22, 2016.
9. Tamara Cibenko, Amelia Dunlop, and Nelson Kunkel, *Human experience platforms: Affective computing changes the rules of engagement*, Deloitte Insights, January 15, 2021.
10. World Economic Forum, *Technology futures: Projecting the possible, navigating what's next*, April 5, 2021.
11. Ibid.

Acknowledgments

Executive editors

Scott Buchholz
Emerging technology research director and Government & Public Services chief technology officer
Deloitte Consulting LLP
sbuchholz@deloitte.com

As a leader and visionary in new and emerging technologies, Scott Buchholz helps clients use technology to transform their organizations, missions, and businesses. He works across industries to provide actionable advice and insights to use technology to improve performance, effectiveness, and efficiency.

He leads Deloitte Consulting's efforts in exploration of quantum computing and related technologies, working to solve customer challenges with these advanced technologies. In his role as CTO for Deloitte Consulting LLP's Government & Public Services practice, he works with government clients to use technology to innovate in their operations, technology, and mission delivery.

Mike Bechtel
Chief futurist
Deloitte Consulting LLP
mibechtel@deloitte.com

As chief futurist with Deloitte Consulting LLP, Mike Bechtel helps clients develop strategies to thrive in the face of discontinuity and disruption. His team researches the novel and exponential technologies most likely to impact the future of business, and builds relationships with the startups, incumbents, and academic institutions creating them.

Prior to joining Deloitte, Bechtel led Ringleader Ventures, an early-stage venture capital firm he cofounded in 2013. Before Ringleader, he served as CTO of Start Early, a national not-for-profit focused on early childhood education for at-risk youth. Bechtel began his career in technology R&D at a global professional services firm where his dozen US patents helped result in him being named that firm's global innovation director. He currently serves as professor of corporate innovation at the University of Notre Dame.

Executive perspectives contributors

STRATEGY

Benjamin Finzi
US and Global Chief Executive Program leader | Deloitte Consulting LLP

Anh Nguyen Phillips
Global CEO Program research director | Deloitte Touche Tohmatsu

Benjamin Stiller
Principal | Deloitte Consulting LLP

FINANCE

Steve Gallucci
US CFO Program leader | Deloitte LLP

Patricia Brown
US CFO Program managing director | Deloitte LLP

Ajit Kambil, PhD
CFO Program global research director | Deloitte LLP

RISK

Deborah Golden
US Cyber & Strategic Risk leader | Deloitte & Touche LLP

Contributors

Anthony Abbatista, Jaime Austin, Stefan Babel, Blair Baillio, Arod Balissa, Amod Bavare, Rupesh Bhat, Douglas Bourgeois, Tobias Brenner, Morgann Carlon, Natalie Chatterton, Anthony Ciarlo, Emily Cole, Morgan Davis, Louis DiLorenzo Jr., Greg Dost, Emma Downey, Michael Eniolade, Michael Fancher, Nairita Gangopadhyay, Andreas Gentner, Adarsh Gosu, Kevin Govender, Stefan Graf, Dorothea Haas, Esther Han, Ariana Hannes, David Harrison, Nikolaus Helbig, Michele Herron, Alexander Hewer, Meirav Hickry, Karen Johnson, Khalid Kark, Tim Kelly, Tovi Kochav, Kelly Komisar, Ed La Hoz Miranda, Matthias Lachmann, Amar Lakhtakia, Rebecca Lalez, Kristi Lamar, Bjoern Langmack, Louis Librandi, Mark Lillie, Daniel Martyniuk, Carey Miller, Simham Mulakaluri, Derek Nelson, Timo Perkola, Dalibor Petrovic, Felipe Piccirilo, Florian Ploner, Dilip Kumar Poddar, Vishal Prajapati, Aparna Prusty, Asish Ramchandran, Hannah Rapp, Alison Rogish, Daniel Rotem, Sanaa Saifi, Peter Sany, Heather Saxon, Rakinder Sembhi, Sofia Grace Sergi, Sandeep Sharma, Sandro Sicorello, Paul Kwan Hang Sin, Nitingaurav Singh, Ranjeet Singh, Nicholas Smith, Tim Smith, Ramona Stordeur, Jan Stratman, Elisabeth Sullivan, Natalie Velazquez, Markku Viitanen, Aman Vij, Jason Wainstein, Jian Wei, Denise Weiss, Shani Weitz, Sourabh Yaduvanshi, Thaddeus Zaharas, Yihong Zeng, and the Knowledge Services team.

Research team

LEADS

Emma Copsey, Ankush Dongre, Mayank Gupta, Rani Patel, Pooja Raj, Katrina Rudisel, and Samantha Topper.

TEAM MEMBERS

Ayshvar Balasubramanyam, Anupama Balla, Srinidhi Bapu, Niko Brammer, Yi-Hui Chang, Krishna Chanthanamuthu, Gurmehar Cheema, Hannah Chen, Soham Dasgupta, Francisco de Ros, Chirag Dixit, Chetana Gururaj, Nidhi Kaushik, Jonathan Key, Ashley King, Mo Koneshloo, Dhir Kothari, Sahil Lalwani, Dong Li, Antaryami Mallick, Swetha Marisetty, Siddhant Misra, Deepashree Mulay, Rutuja Naik, Amruta Pawar, Anna Perdue, Harsh Raman, Vandhanaa Ramesh, Spandana Narasimha Reddy, Nikolaus Rentzke, Prateeti Sarker, Sai Krupan Seela, Bala Seshu Sesham, Kshitij Pratap Singh, Manpreet Singh, Rachel Spurrier, Brendan Stec, Raghul Surendran, Jack Suter, Alap Trivedi, and Falyn Weiss.

Special thanks

Stefanie Heng for grace under fire while masterfully conducting the *Trends* orchestra and managing the dynamic diva duo. Without your ability to keep dozens of plates spinning, we would've crashed and burned many times over. Thank you for all you do!

Doug McWhirter for your infallible leadership and wicked wit. In addition to wrangling words from smacks of SMEs, you grew and cultivated a subtlety of rock star designers and writers who went above and beyond. We appreciate you more than words can say.

Caroline Brown for poise under pressure. We appreciate your continued ability to transform streams of consciousness, reams of research, and an impatience of interviews into brilliant prose, all while dominating on other projects and tutoring teammates.

Adrian Espinoza, Ed Burns, and **Heather Mara** for a fantastic freshman year! Jumping straight into *Trends* is no mean feat. Your fresh perspectives and ideas were deftly transformed into wise words, gorgeous graphics, and a compelling creative vision. Bravo!

Natalie Martella for embracing every opportunity (and sharing levity with your joke-of-the-week). Thank you for coconducting, helping turn the cacophony into a symphony, and leaning into all facets of development, design, and marketing. Huzzah!

Aaron Gano, Abhijith Ravinutala, Kelly Gaertner, and **Maria Wright** for pitching in on all fronts. For relentless research to resounding reviews to intense interviews and more, you helped raise the bar (and the roof). We are beyond lucky to have you on the team!

Alison Cizowski, Cheylin Parker, Mary Hughes, and **Tracey Parry** for your relentless endeavors to get *Trends* to the public. We appreciate your support across all things marketing, communications, and PR!

Aditi Rao, Andy Bayiates, Blythe Hurley, Sarah Jersild, and the entire Deloitte Insights team. For the continued support, patience, and partnership, we thank you and appreciate your drive to improve and evolve *Tech Trends* every year.

Alexis Werbeck, Joanie Pearson, Mackenzie Odom, Matt Lennert, and the Green Dot Agency, thank you for another incredible year of collaboration and bringing our creative vision to life. It gets better and better.

Deloitte.
Insights

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

Follow @DeloitteInsight

www.deloitte.com/us/TechTrends

Follow @DeloitteOnTech

Deloitte Insights contributors

Editorial: Aditi Rao, Blythe Hurley, Andy Bayiates, Aparna Prusty, Dilip Kumar Poddar, Emma Downey, Nairita Gangopadhyay, and Rupesh Bhat

Creative: Alexis Werbeck, Adrian Espinoza, Heather Mara, and Jaime Austin

Promotion: Hannah Rapp

Cover artwork: Bose Collins

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

Copyright © 2022 Deloitte Development LLC. All rights reserved.
Member of Deloitte Touche Tohmatsu Limited