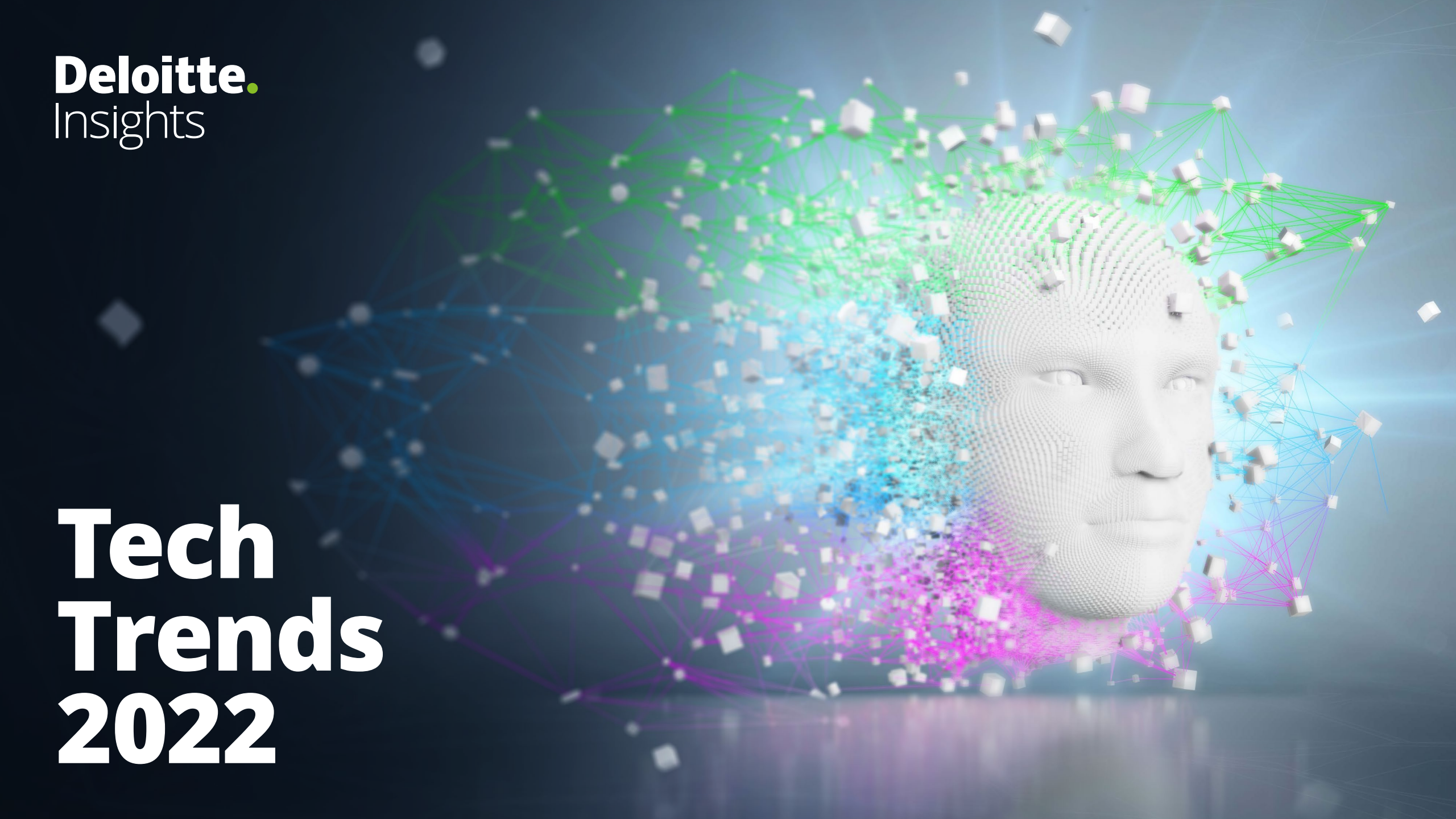
Deloitte.
Insights



Tech Trends 2022

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.

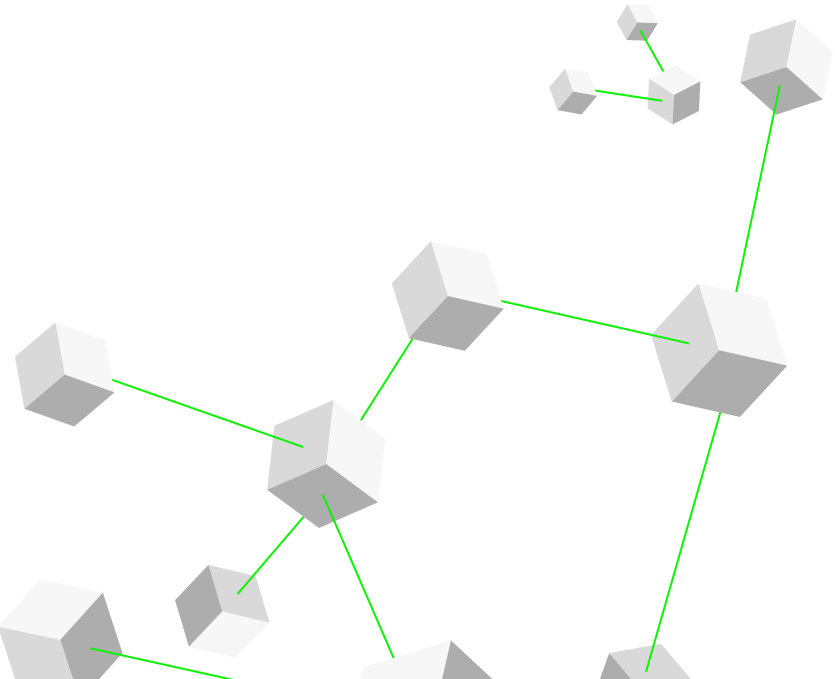
The way forward

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.

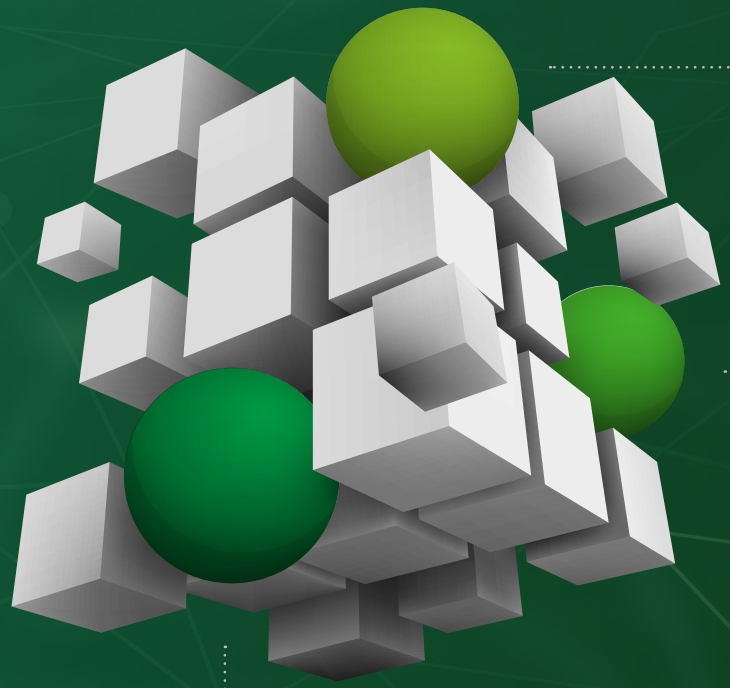
FINANCE

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?



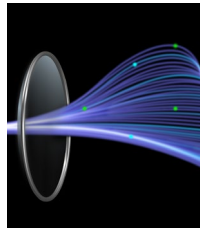
KEY QUESTIONS

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

Sandeep Sharma, PhD

Deputy chief technology officer

Deloitte Consulting LLP

sandeepksharma@deloitte.com

Robert Schmid

Internet of Things practice leader

Deloitte Consulting LLP

roschmid@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.

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

About Deloitte