I'm not a bot

A digital twin is a virtual representation of an object or system designed to reflect a physical object accurately. It spans the object's lifecycle, is updated from real-time data and uses simulation, machine learning and reasoning to help make decisions. The studied object for example, a wind turbine, is outfitted with various sensors related to vital areas of functionality. These sensors produce data about different aspects of the physical object's performance, such as energy output, temperature, weather conditions and more. The processing system receives this information and actively applies it to the digital copy. After being provided with the relevant data, the digital model can be utilized to conduct various simulations, analyze performance problems and create potential enhancements. The ultimate objective is to obtain valuable knowledge that can be used to improve the original physical entity. Although simulations and digital twins both utilize digital models to replicate a system's various processes, a digital twin is actually a virtual environment, which makes it considerably richer for study. The difference between a digital twin and a simulation is largely a matter of scale: While a simulation typically studies 1 particular process, a digital twin can run any number of useful simulations to study multiple processes. The differences don't end there. For example, simulations usually don't benefit from having real-time data. But digital twins are designed around a two-way flow of information that occurs when object sensors provide relevant data to the system processor and then happens again when insights created by the processor are shared back with the original source object. By having better and constantly updated data related to a wide range of areas, combined with the added computing power that accompanies a virtual environment, digital twins can study more issues from far more vantage points than standard simulations can, with greater ultimate potential to improve products and processes. There are various types of digital twins depending on the level of product magnification. The biggest difference between these twins is the area of application. It is common to have different types of digital twins co-exist within a system or process. Let's go through the types of digital twins to learn the differences and how they are applied. Component twins or Parts twins Component twins are the basic unit of a digital twin, the smallest example of a functioning component. Parts twins are roughly the same thing, but pertain to components of slightly less importance. Asset twins When two or more components work together, they form what is known as an asset. Asset twins let you study the interaction of those components, creating a wealth of performance data that can be processed and then turned into actionable insights. System or Unit twins The next level of magnification involves system or unit twins, which enable you to see how different assets come together to form an entire functioning system. System twins provide visibility regarding the interaction of assets and may suggest performance enhancements. Process twins Process twins, the macro level of magnification, reveal how systems work together to create an entire production facility. Are those systems all synchronized to operate at peak efficiency, or will delays in one system affect others? Process twins can help determine the precise timing schemes that ultimately influence overall effectiveness. The idea of digital twin technology was first voiced in 1991, with the publication of Mirror Worlds, by David Gelernter. However, Dr. Michael Grieves (then on faculty at the University of Michigan) is credited with first applying the concept of digital twins to manufacturing in 2002 and formally announcing the digital twin software concept. Eventually, NASA's John Vickers introduced a new term, "digital twin" in 2010. However, the core idea of using a digital twin as a means of studying a physical object can actually be witnessed much earlier. In fact, it can be rightfully said that NASA pioneered the use of digital twin technology during its space exploration missions of the 1960s, when each voyaging spacecraft was exactly replicated in an earthbound version that was used for study and simulation purposes by NASA personnel serving on flight crews. The use of digital twins enables more effective research and design of products, with an abundance of data created about likely performance outcomes. That information can lead to insights that help companies make needed product refinements before starting production Even after a new product has gone into production, digital twins can help mirror and monitor production systems, with an eye to achieving and maintaining peak efficiency throughout the entire manufacturing process. Digital twins can even help manufacturers decide what to do with products that reach the end of their product lifecycle and need to receive final processing, through recycling or other measures. By using digital twins, they can determine which product materials can be harvested. While digital twins are prized for what they offer, their use isn't warranted for every manufacturer or every product created. Not every object is complex enough to need the intense and regular flow of sensor data that digital twins require. Nor is it worth it from a financial standpoint to invest significant resources in the creation of a digital twin. (Keep in mind that a digital twin is an exact replica of a physical object, which could make its creation costly.) Alternatively, numerous types of projects do specifically benefit from the use of digital models: Physically large projects: Buildings, bridges and other complex structures are bound by strict rules of engineering. Mechanically complex projects: Jet turbines, automobiles and aircraft. Digital twins can help improve efficiency within complicated machinery and mammoth engines.Power equipment: This includes both the mechanisms for generating power and transmitting it.Manufacturing projects: Digital twins excel at helping streamline process efficiency, as you would find in industrial environments with co-functioning machine systems. Therefore, the industries that achieve the most tremendous success with digital twins are those involved with large-scale products or projects: Engineering (systems)Automobile manufacturingAircraft productionRailcar designBuilding constructionManufacturingPower utilities The rapidly expanding digital twin market indicates that while digital twins are already in use across many industries, the demand for digital twins will continue to escalate for some time. In 2022, the global digital twins market was projected to reach USD 73.5 billion by 2027.1 The use of end-to-end digital twins lets owners and operators reduce equipment downtime while upping production. Discover a Service Lifecycle Management solution created by IBM® and Siemens. Digital twins are already extensively used in the following applications: Power-generation equipment Large engines, including jet engines, locomotive engines and power-generation turbines benefit tremendously from the use of digital twins, especially for helping to establish time frames for regularly needed maintenance. Structures and their systems Big physical structures, such as large buildings or offshore drilling platforms, can be improved through digital twins, particularly during their design. Also useful in designing the systems operating within those structures, such as HVAC systems. Manufacturing operations Since digital twins are meant to mirror a product's entire lifecycle, it's not surprising that digital twins have become ubiquitous in all stages of manufacturing, guiding products from design to finished product, and all steps in between. Healthcare services Just as products can be profiled by using digital twins, so can patients receiving healthcare services. The same type system of sensor-generated data can be used to track various health indicators and generate key insights. Automotive industry Cars represent many types of complex, co-functioning systems, and digital twins are used extensively in auto design, both to improve vehicle performance and increase the efficiency surrounding their production. Urban planning Civil engineers and others involved in urban planning activities are aided significantly by the use of digital twins, which can show 3D and 4D spatial data in real time and also incorporate augmented reality systems into built environments. A fundamental change to existing operating models is happening. A digital reinvention is occurring in asset-intensive industries that are changing operating models in a disruptive way, requiring an integrated physical plus digital view of assets, equipment, facilities and processes. Digital twins are a vital part of that realignment. The future of digital twins is nearly limitless because increasing amounts of cognitive power are constantly being devoted to their use. So, digital twins are constantly learning new skills and capabilities, which means they can continue to generate the insights needed to make products better and processes more efficient. In this article on transforming asset operations with digital twins, learn how change impacts your industry. Digital transformation in banking is the act of integrating digital technologies and strategies to optimize operations and enhance personalized experiences. Across the financial services industry, this process can occur by breaking down data silos and reimagining the customer experience. The world is rapidly changing to be more digitally focused, especially in the banking industry. Traditional banks are undergoing major digital transformations in order to meet the needs of new customers and existing customers seeking a more tailored and individualized banking experience through digital channels. To make it possible, banks and financial institutions must take on a digital transformation strategy that puts customer experience first by analyzing, interacting and understanding customer needs. Digital transformation isn't new to the banking sector, but it has become more relevant as fintech and new operating models have gained in popularity. Traditional banks must keep up with the changing market and ever-evolving customer needs, such as the drive toward using mobile apps or websites to perform transactions. These types of technology are part of the omnichannel strategy banks are using to break down data silos and reimagine the customer journey. With the more recent shift toward automation, banks and financial service providers need to modernize their banking strategies. The growing demand for artificial intelligence (AI), Internet of Things (IoT), and blockchain are among the other technologies banks must consider when creating a digital transformation strategy. Customers are seeking digital approaches to managing their accounts, prioritizing personalized product experiences, transparency and security—all in real-time. Mobile devices drive this digital transformation trend, along with customers increasing need to stay constantly connected. The only way to meet the customer needs is through a digital transformation journey. This journey harnesses customer data to analyze behavior patterns, enabling businesses to align more relevant products and services with their customers' needs. Customer journey: Considering the more customer-centric approach and by using data and other new technologies to tailor banking services to the individual customer. Modernized infrastructure: New technologies, such as automation and AI can streamline internal operations and ultimately boost efficiency and give these banks and financial service providers the competitive advantage. Data analytics: By using advanced data analytics tools, banks can have more informed and strategic decision-making. Breaking down these data silos provides more opportunity for better risk management and innovation. Security measures: A part of digital banking transformation is adopting new and advanced cybersecurity measures that better protect sensitive customer data. Online banking and digital services bring about a new layer of security concerns. With advanced technology in place, banks can bring in fraud detection measures and ensure that regulatory compliance is met. Digitization: The digital era is upon us and it's on the financial sector to align with these other sectors taking the digital-forward approach. For these reasons digital transformation initiatives are so important, such as partnering with fintech startups or open banking frameworks that aim to expand services for stakeholders. For a successful digital transformation to take place banks must take advantage of the latest digital technology available. Here are some of the most common existing technologies within the banking and financial services sector. Application programming interfaces (APIs): An API is a software interface that allows for two or more software applications to integrate data services and capabilities, instead of having to develop them from scratch. Which allows for better connectivity for businesses to their new customers and partners? Furthermore, they can create new products and services for their customers and improve overall operational efficiency. Cloud computing: Cloud computing technology is the on-demand access of computing resources, which banks and financial service providers have come to use and accept. The cloud environment allows for better operations and a more flexible infrastructure that's agile and scalable. AI and machine learning (ML): The AI and ML technologies are being used for several transformation efforts, including analyzing significant datasets, automating certain processes and improving the user experience through personalized services. AI in particular is used in banking through online assistants and chatbots that can address basic customer issues. Separately, an advantage of using ML in banking is that it makes it easier to track changes in user behavior and detect fraudulent activity faster. Internet of Things. (IoT): IoT refers to a network of physical devices, think wearable smartwatches or smart thermostats that are embedded with sensors and software that allows them to collect and share data. For banks, this smart connectivity has allowed customers to make instant contactless payments and interact with their accounts in a mobile banking capacity. The IoT can also be thanked for bringing risk management and advancements in the authorization process more than ever. Blockchain: The transparent and information-driven nature of blockchain makes it a trending technology for banks and financial service providers. It has resulted in more secure data transactions and an enhanced interface that meets and goes beyond customer expectations. Today, customers trust blockchain solutions and find it to be a more transparent way of operating business models. The changing market and push toward new technology make it imperative to evolve. While the digital transformation process can be intimidating, with the right resources and assistance, banks can see the tremendous benefits from the transformation journey. As your bank or financial service provider begins the transformation process, here are some basic steps to follow: Establish business objectives Have goals in mind before setting out on a transformation journey. It's important for the transformation team to lay out their business and technical objectives and understand what they want to gain from the transition. Action item: Create a list of priority objectives to start and then tailor that list as the bank or financial institution leaders see fit. Evaluate your current technology Take stock of all the current systems and products that your bank is using. Once the list of all current systems has been made, evaluate them based on how each is working or not working toward your business goals. It's important to be transparent about your bank's process and be open to modifying it to fit the digital landscape. Action item: Be clear about your processes. List out which processes are necessary for your transformation, while also considering constraints including cost and timeline. Align scope and customer needs To understand what your clients need next, take back a step and evaluate how you're taking stock of current clients. Use data analysis to understand how you are segmenting and collecting data on clients. Use the data to understand which products are selling and which digital services are most popular to the clients. Action item: Make a plan so that you are targeting consumers more likely to use digital services. Ensure that your data is working for your business needs. Marketing teams can have a much more targeted approach once these consumers are identified and understood. Assess priorities Be realistic about your resources and what your organization can handle, in terms of both monetary and human resources. Define your target architecture and early proofs of value to measure achievements toward your business goals. Action item: Write out your objectives; list out ways in which you can enable your institution to make incremental changes at first. Early wins, even small ones, help with transformation buy-in and momentum. Present business case Once all transformation preparation has been made, present the business case for core systems transformation to key stakeholders. The business case must be delivered to the C-suite and board of directors, if relevant, for sign-off. Once you have signed off, proceed with operationalizing the roadmap and strategy for a full transformation. Action item: Prepare your presentation for key stakeholders. Be prepared to defend the transformation needs you have found and laid out. Digitization in the banking system is complex and goes much further beyond just moving a traditional bank to an online banking system. The transformation process can bring about new opportunities for businesses of all sizes and bring forth banking solutions that provide greater customer satisfaction. Here are some of the greatest benefits from digital transformation in banking and financial services. More customer-focused investment banking: Digital transformation in investment banking is more customer-focused than ever before. Because digital transformation in investment banking has replaced investment banks with small investors, the focus is now on short-term goals and all on one-digital platform. Offerings and technological decisions are now based on customer profiles.Easier compliance: By making the switch to a modern financial management system, banks and financial service providers can stay compliant. There are automated processes that can help employees allocate less time doing tasks like auditing reports and instead focus on the work that matters most. If a bank is on a cloud-based system, it provides timely updates and keeps up to date on regulations automatically.Access new clients: A digital-native environment makes attracting customers easier by being upfront about their services and what they can provide. By going digital, banks are making customer acquisition much easier with expanded services and 24x7 account access.Enhanced security: With the growth of digitization, comes the challenge of data security and businesses securely managing customer data. Thankfully, there are sophisticated software development services available to protect your customers personal information and save their accounts from being hacked or scammed.More personalized banking: A digital transformation helps banks and financial institutions to hone in on exactly what a customer needs and wants. There is no longer the need to assume what a customer wants, with new technology, a bank can know exactly what it is the customer expects of them. Banking is no longer just a weekly practice, it's a daily act that requires a fast and secure ecosystem that customers can trust. As the pace of digital transformation accelerates in the manufacturing and engineering industries, two concepts have gained significant traction: digital twins and digital threads. Both concepts refer to digital representations of physical objects, but they serve different purposes and offer companies unique advantages. Here, we will compare digital twins and digital threads, and discuss potential use cases and benefits. A digital twin is a digital replica of a physical object or system, complete with all the design and operational data of the physical object, including geometry, performance data and behavior models. The purpose of a digital twin is to simulate the behavior of equipment in real-time, allowing engineers and operators to monitor performance and identify system issues/anomalies.Digital twin technology uses Industrial Internet of Things (IIoT) sensors, machine learning and simulation software to collect product data and generate accurate models. Teams can then use the models to predict maintenance needs, simulate changes to the system and optimize processes (e.g., safety protocols, reporting procedures, manufacturing processes, etc.).For example, a digital twin of a wind turbine can simulate the impact of changing wind speed and direction on the turbine's performance, helping operators make informed decisions about maintenance and energy production. A digital thread is a digital representation of a product's lifecycle, from design to manufacturing to maintenance and beyond, providing a seamless flow of data that connects all aspects of the lifecycle. The purpose of a digital thread is to provide a complete and transparent view of manufacturing systems, enabling efficient collaboration and decision-making across all stages of the process.Digital threads use a variety of technologies, including computer-aided design (CAD) software, product lifecycle management (PLM) systems and Internet of Things (IoT) sensors, to collect and share data across workflows. Digital thread technology optimizes traceability, providing a way to track asset progress and ensure that all stakeholders are on the same page throughout the production process. For example, aerospace companies can create a digital thread to help assemble aircraft with digital engineering. Production teams utilize 3D-model-based systems to guarantee that aircraft are built exactly to engineering specifications and rely on the digital thread to track progress and identify issues and inefficiencies during production. Both digital twins and digital threads utilize virtual representations of real-world assets and processes, but they offer distinct capabilities.Digital twins are scalable, but only to a point. Digital twin technology collects real-time data from a single source/asset. And although a digital twin concept can connect to other twins to simulate entire digital environments, they are most useful in evaluating a specific production environment. A digital thread concept, on the other hand, is limitlessly scalable. Digital threads can connect to (almost) any other enterprise system, including digital twins.As such, digital thread technology may be best suited for operations and/or circumstances where data must be gathered from an array of departments, devices, systems and processes. On the contrary, digital twins will better serve operations that rely primarily on repetitive machine processes within a specific production environment.Both digital twins and digital threads centralize data to some extent. Both collect comprehensive sensor data and aggregate and store that data in an easily accessible data hub. However, digital threads enable teams to take data from digital twins and other sources and centralize the data flow across departments and production silos so that the entire company can access the same information. Data attached to a digital thread also tends to be more consistently accurate, because the automation features of a digital thread concept eliminate the need to manually transmit information between departments and workflows. Digital twins and digital threads help organizations increase system efficiency, reduce production costs, improve product design and limit system downtime. However, the impact of each technology will vary depending on manufacturer needs.Digital twins allow manufacturers to do the following:Engage in responsive monitoring in real timeConduct proactive risk assessments and utilize predictive troubleshooting for organizational assetsAccelerate innovation using digital models and digital mirroringDigital threads help manufacturers in the following ways:Build more agile operations by facilitating a continuous, synchronized data flowIncrease interdepartmental collaboration across assets and systemsOptimize connectivity between manufacturing and engineering processesStreamline product development to reduce production time and get products to market fasterEnsure regulatory compliance by tracking the entire product lifecycle, including design decisions, engineering changes and maintenance records Digital twins and digital threads are essential tools for companies looking to start or accelerate a digital transformation. Using advanced technological tools like IBM Maximo can help organizations get there faster. IBM Maximo is a comprehensive enterprise asset management system that helps organizations optimize asset performance and streamline day-to-day operations. Using an integrated AI-powered, cloud-based platform, IBM Maximo offers comprehensive CMMS capabilities that produce advanced data analytics and support manufacturers looking to make informed decisions about system performance and optimization. Using IBM Maximo software, especially as a complement to existing enterprise resource management (ERP) systems or a manufacturing execution system (MES), can help your facility gain a competitive edge in today's ever-evolving manufacturing marketplace. A digital identity is a profile or set of information tied to a specific user, machine or other entity in an IT ecosystem. Digital IDs help computer systems distinguish between different users for access control, activity tracking, fraud detection and cyberattack prevention. In most systems, an entity's digital identity is made of their unique attributes. Together, these attributes form a record that verifies the entity's identity and distinguishes them from other entities. For example, a human user's identity in a corporate network might include identity information such as their social media handles, Social Security number and network username. Verifiable digital identities are the foundation of authentication and authorization, the processes that IT systems use to verify users and grant them appropriate access. Both human and nonhuman users need digital identities to interact with digital services and one another. Trusted digital identities allow people, machines, apps and service providers to be sure that the entities they interact with are who they say they are. Digital identities also allow systems to monitor activity and determine which entities are taking which actions. Because of their importance to the digital world, digital identities are a major concern for organizations today. A study for the Identity Defined Security Alliance found that more than half of organizations (51%) see managing and securing digital identifications as one of their top three priorities.1 Stay ahead of threats with news and insights on security, AI and more, weekly in the Think Newsletter. There are multiple types of digital identities—not only for people, but also for devices, services and other digital entities. Human digital identities are the digital identities that correspond to human users in a system. A human digital identity might include information such as age, driver's license, Social Security number or biometric data such as fingerprints and facial recognition scans. Humans use their digital IDs to access digital resources, such as logging in to a bank account online or retrieving sensitive assets on a corporate network. Machine identities correspond to nonhuman entities such as apps, bots, Internet of Things (IoT) nodes and other devices. They often use unique identifiers such as certificates or tokens to authenticate and distinguish themselves. Just like a human user's digital ID, a machine's digital ID allows it to access certain digital resources, such as a business app fetching sensitive data from a cloud database. Federated identities enable individuals to use their digital identities across multiple systems and services. Federated identities are essentially a type of user or machine identity that is not limited to one system. They give the user the added convenience of not needing to create a different identity for each system. Interoperability—a standards-based approach to enabling different IT systems to exchange data—helps enable identity federation. Digital identities play a key role in the identity and access management (IAM) systems that enterprise organizations use to enforce cybersecurity measures and control user access to digital resources. When a new user needs access to a system—a new employee on a company network or a new server in a data center—the user must establish a distinct digital identity in that system. The IAM system then uses these distinct digital IDs to monitor user activity and apply tailored permissions. When a user requests access to a digital asset, they must authenticate themselves with the IAM system. Authentication entails submitting some credentials—such as a username and password, date of birth or digital certificate—to prove the user is who they claim to be. For extra security, some IAM systems might use multifactor authentication (MFA), which requires users to provide more than one authentication factor to prove their identities. When the user passes authentication, the IAM system checks the permissions associated with their unique digital identity and grants only those approved permissions. In this way, IAM systems keep out hackers while helping ensure that each individual user has the exact permissions they need for their tasks. In a single sign-on (SSO) system, a user can use one digital identity to access multiple apps and online services. The SSO portal authenticates the user and generates a certificate or token that acts as a security key for various interconnected resources. Enhanced cybersecurity Digital identities help protect computer systems from threat actors, fraud, identity theft and other unauthorized activities. According to the X-Force Threat Intelligence Index, the theft of valid accounts is the most common way that cybercriminals break into victim environments, accounting for 30% of all incidents. Digital identities can help close vulnerabilities in the identity layer and strengthen data protections against identity-based attacks in a few ways. Digital identities make it easier for organizations to track user activity. Not only can they distinguish between authorized and unauthorized users, but they can also spot suspicious behavior associated with authorized users' digital identities, which can signal an account takeover in progress. Extra measures, such as MFA and time-based credentials, can also help safeguard digital identities from being stolen or misused. These added layers of security can help drive revenue rather than drain budget. An IBM Institute for Business Value study found that 66% of operations executives view cybersecurity as a revenue enabler. Promoting trust Trust is key to enabling collaborative workflows among internal staff, customers, service providers and external partners. A strong digital identity management system helps users trust that the people, machines and services they connect with are authentic and reliable. Artificial intelligence (AI) can help speed up digital identity verification processes by analyzing huge datasets of digital identifiers, such as facial features, fingerprints or retina scans. This helps streamline and strengthen identity verification, further promoting trust within computer systems. Flexibility of location Part of the power of cloud services is that they can be accessed from almost anywhere. But strong identity verification processes are required to prevent unauthorized and fraudulent access. With the rise of remote work and cloud computing, users are increasingly distributed, and so are the resources that they need to access. A verified digital identity can substitute for—and offer as much security as—swiping a chipped ID card on site or showing a driver's license or passport. Users can control their identities Some decentralized digital identity systems allow users to create their own portable digital identities and store them in digital wallets. Such ecosystems give identity control to the individual and take the onus of managing the identities off service providers. To verify users' digital identities, organizations can check their credentials against a shared trust registry. There is a vast array of use cases for digital identities across industries, with many supporting how users and applications interact with cloud resources.   Governments often use digital credentials to streamline and secure the delivery of government services. Secure digital identities enable citizens to verify themselves so they can collect benefits and file taxes, and governments can trust that these citizens are who they say they are.   Digital identities enable patients to securely share health data with their providers, making it faster and easier to get multiple opinions before determining a medical treatment plan. Providers can use digital identity solutions to verify insurance coverage, monitor health devices and help comply with rules such as the Health Insurance Portability and Accountability Act (HIPAA). Digital identities enable sellers to deliver better customer experiences tailored to individual users based on their personal data. For example, digital identity systems enable customers to store payment data for later purchases, while retailers can use the order history associated with unique identifiers to generate personalized recommendations. Digital HR refers to the transformation of traditional human resources (HR) functions through the adoption of digital technologies, data analytics and automation. Digital HR is the evolution of HR from paper-based, manual processes and systems to technology-driven approaches. Often organized alongside an enterprise-wide digital transformation, digital HR practices can increase efficiency, improve decision making and create better employee experiences. Traditionally, HR professionals receive traffic in large amounts of data from across channels, including internal employee communications and external candidate information. Local workforce regulations govern many HR functions, complicating compliance for global firms. By digitizing and unifying multiplatform HR functions, organizations reduce these manual efforts and increase productivity across an organization. But a digital transformation for HR, designed correctly and deploying key technologies, can also create new paradigms for HR departments. Rather than simply digitizing HR processes, a digital HR transformation rethinks how HR operates by using tools such as cloud platforms, artificial intelligence (AI), analytics and automation. HR departments, empowered to make data-driven decisions and spend more time on creative or intimate tasks, can become drivers for a positive company culture. In this context, digital HR represents more than a technological upgrade; it fundamentally changes how organizations attract, develop, engage and deploy talent to create business value. Digital HR processes can also be a critical facet in the change management process, creating more agile organizations capable of absorbing new processes quickly. In recent years, new technologies such as agentic AI and generative AI have vastly increased departments' capacity for scalable and highly personalized experiences, ushering in an era of human-focused, experience-oriented HR. Increasingly, HR tech is facilitating a future of HR in which personnel leaders evolve from service providers to architects of the employee experience. By working in collaboration with technology, they can enhance an organization's potential holistically. Discover expertly curated insights and news on AI, cloud and more in the weekly Think Newsletter. Redesigning HR functions with digital solutions can create more loyal and engaged employees—which in turn converts to increased profit. According to the IBM Institute for Business Value, organizations that nurture top employee experiences outperform by 31% compared to other enterprises. There are many benefits to implementing a digital HR process. With key technological integrations, HR departments can create seamless and personalized experiences for their employees throughout their time with the organization. Self-service portals and AI-powered assistants empower employees to manage their own informational requests and administrative needs without dependency on HR staff. This process ultimately helps resolve issues faster and allows HR leaders to focus on more human-centric tasks. With HR-specific AI agents, employees can receive proactive and hyperpersonalized communications tied to major life events or career goals. These agents help streamline employee communications within their enterprise and provides them with exactly the information they need, when they need it. The automation of administrative tasks can dramatically reduce the time HR teams spend on routine activities. For example, digital workflows streamline processes such as paid time off (PTO) approvals that might have previously required several manual interventions. Centralized digital documentation can eliminate paper-based record-keeping, reducing costs and improving accessibility across an organization. For example, in one pilot, IBM created a digital worker to help its own HR department complete previously manual data-gathering and data-entry tasks. This process helped save employees 12,000 hours over a single quarter. Digital HR platforms and dashboards can generate comprehensive workforce analytics, informing strategic talent management and resource allocation decisions. For example, AI-enabled screening mechanisms might help HR leaders proactively identify and rank potential candidates based on predefined metrics, while internal analytics tools help departments run promotions fairly. These sophisticated analytic systems can provide managers with up-to-date insights, improving day-to-day decision making and creating more agile organizational structures. Digital transformation and the unification of cross-departmental data that it often involves enables HR to more directly contribute to business objectives. This approach might include collaborating to more accurately plan for personnel needs or helping to design training programs based on HR data. By using technology in HR operations, HR departments can shift from administrative bodies to strategic enterprise partners, increasing productivity and innovation across an organization. Digital HR services can allow businesses to quickly adapt to changing business conditions and market disruptions. As digital systems are often cloud-based and can accommodate scaling up or down, they are more agile than traditional HR models. This flexibility reduces the cost of expansion and yields a more resilient organization. Digital HR systems enhance data security and regulatory compliance compared to fragmented, paper-based systems. Automated compliance workflows can flag potential compliance issues before they arise, reducing risk across employment and data privacy laws. For global organizations, digital HR platforms can automatically apply appropriate rules based on employee location, helping ensure compliance with varying local regulations. Furthermore, centralized employee records can ensure sensitive information is only available to authorized stakeholders. And cloud-based platforms allow for superior encryption practices, preventing security breaches. Digital tools can transform the recruitment process, easing the burden of sifting through thousands of resumes and matching candidates with the most appropriate position. For example, intelligent sourcing tools analyze job requirements and automatically identify potential candidates, while AI-powered screening technologies evaluate applications against a range of criteria. These tactics can reduce bias while identifying the candidates most likely to succeed. Also, AI and automation technologies can handle routine tasks such as interview scheduling and meeting summarization. These features provide HR leaders with critical data and allow them to focus on the human-centric aspects of the candidate experience. Similarly, digital onboarding significantly reduces friction and improves the employee experience starting from a team member's first day on the job. AI-powered tools guide new hires through paperwork, account setup and orientation materials at their own pace. While personalized learning paths provide role-specific information based on a nice hire's position and background. Using onboarding analytics, enterprises can track engagement and progress, allowing for intervention should issues arise. Digital and AI-powered HR platforms can provide real-time, continuous and proactive performance development for an entire workforce simultaneously. For example, real-time goal management systems enable the creation and tracking of objectives over time, while feedback tools can collect perspectives from a range of stakeholders to provide comprehensive performance insights. Simultaneously, advanced people analytics identify performance patterns across teams and departments, providing suggestions to improve outcomes. Natural language processing (NLP), along with sentiment analysis tools, can reveal broad themes and insights that might not be recognizable to individual managers. Such performance data can be integrated with compensation and development systems to create a coherent, business-specific talent management process. Today's learning experience platforms can create personalized trainings and content based on an individual's role, career goals and learning preferences. These platforms can even proactively scan employee communications on social media platforms, like LinkedIn, to identify internal opportunities and recommend trainings. In some applications, personalized, AI-generated simulations facilitate hands-on learning opportunities, allowing employees to practice new skills or interact with mock customers. And by integrating learning, performance and workforce planning systems enterprises can proactively develop individual education plans to better align with broader business strategies. Digital engagement strategies measure, analyze and continuously improve the employee experience. These initiatives—which blend proactive communication and internal analysis—streamline administrative tasks and increase employee satisfaction by reducing friction across an organization. They also allow HR leaders to spend more time crafting creative engagement initiatives. These initiatives can also provide business leaders with the tools to detect potential roadblocks before they arise. Sentiment analysis of digital communications can identify potential engagement issues before they appear in more formal values, while digital collaboration tools strengthen connections between colleagues despite physical distance. Digital well-being tools can support holistic employee health through activity tracking and personalized recommendations and recognition platforms improve company culture regardless of employees' geographic location. Using intelligent analytics built into HR systems, organizations can identify the specific factors that drive engagement for different employee segments, enabling personalized and targeted interventions rather than a one-size-fits all approach. AI assistants, a more intelligent and sophisticated form of chatbot, understand natural language commands and use a conversational AI interface to complete tasks. They can be integrated into digital HR solutions to quickly retrieve specific company information for an employee, answer questions about specific policies or complete administrative requests based on natural language. AI agents, proactive systems that operate independently to meet specific goals, augment the HR process in myriad ways. For example, they can manage time off and payroll processes, administer benefits such as healthcare, craft offer packages and offer tailored guidance during the employee onboarding experience. IBM's internal AskHR digital assistant automates over 100 processes across the organization, handling over 1.5 million employee conversations every year. Generative AI is used in digital HR systems to create new content and generate insights. Advanced language models assist with the development of job descriptions and personalized candidate communications. For employee communications, generative AI can draft announcements, policies and learning content with a consistent tone. Often, generative AI is integrated with other platforms or systems to create robust HR-focused workflows. Human resources information systems (HRIS), a key HR technology, serve as the digital foundation for employee data management, providing a single source of truth for workplace information. Typically cloud-based, these platforms offer scalability and accessibility from anywhere, reducing the cost of maintenance for on-premises systems. Many solutions incorporate comprehensive integration capacities, allowing seamless data exchange with other enterprise systems. Analytics platforms transform workplace data into actionable insights through pattern recognition and predictive modeling. Sentiment analysis of survey data and digital communications can provide early warning of engagement issues or workflow bottlenecks. Meanwhile, natural language processing (NLP) can extract insights from unstructured data sources including performance reviews and exit interviews. AI-powered candidate screening tools evaluate resumes against job requirements, identifying promising candidates from large applicant pools or external sources such as LinkedIn. Candidate relationship management systems support HR leaders in nurturing relationships with potential hires, help ensure compliance and aid departments to effectively manage candidate data. For example, the ceramics and glass manufacturer Corning recently integrated SAP SuccessFactors to help attract new talent and reduce costs for a workforce spread between 22 countries and 12 languages. The organization was quickly able to advertise 1,000 job vacancies and attracted 80,000 global job applicants. Continuous performance management systems enable regular feedback, goal tracking and development planning. Meanwhile, digital coaching systems—often based on AI technologies—connect employees with resources based on their development needs and career aspirations. Skills management platforms track capabilities and skills across the workforce, identifying opportunities for internal mobility and targeted development. Learning experience platforms curate personalized development content from multiple sources based on individual needs and preferences. In one recent instance, IBM's event management team for enterprise learning used digital HR solutions to optimize the planning, scheduling and delivery of learning events. This initiative created 8,000 discrete learning opportunities to the workforce over a period of only six months. Digital workplace solutions create a series of unified employee experiences across HR communications. Self-service portals can provide intuitive, continuously accessible interfaces for accessing HR information and services. Personalization engines, which rely on AI and machine learning, deliver targeted communications based on employee profiles and behaviors. To effectively design and deploy an effective digital HR strategy, it's often useful to begin with a comprehensive assessment of current HR processes alongside a transformation's strategic objectives. This process might include developing a clear vision for digital HR that articulates how the technology transforms the employee experience and operational efficiency. It can also be necessary to create a long-term roadmap for how a digital HR transformation aligns with broader business goals. Typically, organizations that approach digital HR as a series of targeted and isolated implementations generate less value than those organizations that integrate solutions holistically across a department. Thoughtfully designed digital HR processes augment and compliment human HR functions and address specific user needs rather than system capabilities. Essentially, successful digital HR initiatives are designed around delightful user experiences. The user, rather than the technology, should come first. Before planning an HR transformation, it's often useful to conduct thorough research with employees to understand their expectations, challenges and preferences around HR interactions. Organizations that focus exclusively on efficiency run the risk of saving HR time but creating frustration for employees and managers. By involving employees in the design process early, HR leaders also pave the way for enthusiastic employee participation and create advocates for digital transformation initiatives in the future. A digital transformation is a good opportunity to fundamentally rethink how HR delivers services across an organization. Designing such a system often involves redefining roles across an enterprise to emphasize data analysis, employee experience design and technology enablement rather than administrative processing. It can also be useful to create cross-enterprise teams that bring together HR, IT and enterprise leadership to address employee experience holistically. By using digital capabilities as an opportunity to reimagine systemic operating models, enterprises can consolidate fragmented processes and ultimately increase HR's value across an organization. By necessity, reimagining the enterprise operating model often includes upskilling and reskilling HR professionals and developing new capabilities in digital literacy, change management and analytics. Over the course of a digital HR transformation, business leaders should think critically about how to introduce new tools to their workforce—and create a roadmap for building digital literacy. This initiative might include dedicated learning opportunities that help HR professionals understand how best to work alongside digital workers and embrace the more creative aspects of their jobs. Reliable, well-organized and transparently collected data is a critical component of a digital HR transformation. A successful initiative includes a comprehensive data strategy that captures enterprise- and function-specific information. AI tools trained on clean and targeted data vastly outperform generic models. For tools, such as AI agents, that might require third-party datasets to perform their intended role enterprises should also carefully vet integrations to help ensure functionality and consistency. As in any digital initiative, building an effective and reliable data governance plan is key. This strategy might mean establishing clear policies around data ownership, access rights and retention periods. Often, a digital HR transformation needs an investment in cybersecurity infrastructure capable of both housing and securing sensitive employee data. By creating robust security protocols, organizations protect sensitive employee data and retain compliance while enabling appropriate access. Data quality standards and regular updates help ensure that analytics and AI tools are based on accurate, consistent information. Transparency practices help employees understand what data is being collected about them and how it is uses, as well as maintaining compliance with evolving regulations. Sign In or Register to comment. Digital transformation is a business strategy initiative that incorporates digital technology across all areas of an organization. It evaluates and modernizes an organization's processes, products, operations and technology stack to enable continual, rapid, customer-driven innovation. Today customers expect to be able to conduct their business, do their work and live their lives by using the latest technology advances. They expect this ability from wherever they are, anytime they want, by using the device of their choice and with all the supporting information and personalized content they need close at hand. The ultimate goal of digital transformation is to meet these expectations. Every organization's digital transformation implementation is different. It can begin with a single focused technology project, or as a comprehensive enterprise-wide initiative. It can range from integrating digital technology and digital solutions into existing processes and products, to reinventing processes and products or creating entirely new revenue streams by using still-emerging technologies. But experts agree that digital transformation is as much about business transformation and change management as it is about replacing analog processes or modernizing existing IT. While often led by a company's chief information office (CIO), it requires the entire C-suite to align on new technologies and data-driven methodologies that can improve customer experience, empower employees and achieve business goals. But, most importantly, companies should create a digital transformation framework and monitor improvements through tracking key performance indicators (KPIs) to see if the work produces results. The earliest, headline-making examples of digital transformation—Uber, AirBnB, Netflix—used mobile and cloud computing technologies to reimagine transactions and, sometimes, disrupt entire industries. The COVID-19 pandemic drove transformative innovations to better support remote and hybrid work. Today, organizations are applying artificial intelligence (AI), automation and other technologies to streamline workflows, personalize customer experiences, improve decision-making, and respond more quickly and effectively to market disruptions and new opportunities. Digital transformation can help companies increase customer loyalty, attract talented employees, foster competitive advantage and build business value. McKinsey research found that between 2018-2022, digital leaders achieved about 65% greater annual total shareholder returns than digital "laggards."1 In digital transformation, domains are essentially targets or levers for transformation. Most digital transformation strategies target one or more of these domains: Business and operating modelsProcessesProductsEmployee experienceCustomer experience Business model transformation is a fundamental change in the way that an organization delivers products, services and value to its customers, investors or stakeholders. Examples include: Delivering video through digital streaming, instead of physical disks (Netflix, Hulu) Enabling anyone with a car to make money driving, without purchasing a medallion (Uber, Lyft)Allowing customers to deposit checks without visiting the bank (mobile deposit) Organizations pursue business model transformation for any number of reasons—for example, to meet changing customer expectations, boost flagging sales, or differentiate themselves in a highly competitive market. They might also see a chance to disrupt a market or industry in their favor with a new business model—or have a need to respond to a disruptive competitor. While business model transformation grabs the headlines, business process optimization is an increasingly common digital transformation driver. Process optimization can include: Consolidating isolated or redundant workflowsCreating intelligent workflows by using AIReplacing manual tasks with AI and automation Process optimization can help organizations lower costs, reduce waste (time, effort and materials), make better use of human capital, and help all stakeholders make smarter decisions faster. Organizations are incorporating digital innovation into their products, and into the way their products are developed, produced and delivered. The most obvious examples involve the embedding of digital technology into everyday products that meet customer needs. Automobiles, for instance, are continually transformed in this way. Innovations range from the ability to view and operate a smartphone from a car dashboard, to sensors that prevent crashes and unintended lane changes, to vehicles that incorporate computer vision, geolocation, machine learning and robotic process automation (RPA) to operate with minimal or no human intervention. By implementing Internet of Things (IoT), operational technology and automation on the factory floor, manufacturers can speed production, reduce errors and defects and eliminate manual labor. By adopting agile or DevOps practices organizations can speed software development. Companies can also add value and competitive differentiation by offering technology alongside their existing services—witness the tracker apps offered by shipping companies and pizza vendors. Employee experience is a holistic approach to talent management that helps ensure that employees have the tools the need to succeed and thrive at work. Employee experience certainly impacts employee recruitment, morale, productivity and retention, but it can also have a direct impact—positive or negative—on customer experience, business performance and brand reputation. Digital transformation efforts to improve employee experience can include: Innovating user experiences for internal systems such as onboarding applications, employee benefits portals and internal communicationsProviding access to popular messaging and collaboration tools Supporting work from home (WFH) or remote work without sacrificing capabilities or productivity Enabling employees to connect securely to corporate resources with the devices they prefer, including their own mobile devices or computers, by using 'bring your own device' (BYOD) policies and initiatives Customer experience, or CX, is the sum of customers' perceptions resulting from all their interactions with a business or brand—online, in-store and in day-to-day life. In the end, all digital transformation journeys lead to the customer experience domain. Continually improving the customer experience is a competitive imperative for most organizations. In the digital age, continually improving the customer experience requires continual digital innovation. It's not just that customers expect to be able to do business anytime, anywhere and on any device—today customers depend on it. They plan their mornings knowing their phones tell them exactly how long it takes to drive to work, and their evenings knowing they can meet the food delivery driver at their door. They ignore customer service call center hours, knowing they can get answers 24/7 from a chatbot. They stop saving receipts knowing that they can download their bank and credit card history at tax time (or anytime). Customers count on these and scores of other digital innovations, and they are ready to count on new ones. Successful digital transformation positions organizations to anticipate and deliver the next innovations and experiences customers will want. Virtually any digital technology can play a role in an organization's digital transformation strategy, but these technologies are most closely associated with transformation initiatives. Cloud computing The original digital transformation enabler, cloud computing enables organizations to use the latest IT technologies, boost efficiency and scale with demand while managing costs. A hybrid cloud infrastructure, combining orchestrated public cloud and private cloud resources from multiple vendors, provides the application portability, vendor flexibility and IT agility needed for enduring digital transformation success. Mobile technology Customers' dependence on mobile devices drove the earliest digital transformation initiatives, transformed existing business models (for example mobile tickets and wallets) and created entirely new ones (for example, Uber). Today customers insist on doing more business through mobile apps, whether simply ordering lunch or dinner from their favorite restaurant, or managing their banking and investments. Internet of Things (IoT) The Internet of Things (IoT) is the universe of devices equipped with sensors that collect and transmit data over the internet. IoT devices are where digital technology meets physical reality. Applications like supply chain logistics and self-driving cars generate real-time data that AI and big data analytics applications turn into automation and decisions. Artificial intelligence (AI) and machine learning AI and machine learning enable a computer or machine to mimic the capabilities of the human mind. AI learns from examples, recognizes objects, makes decisions and quickly processes large tasks. Generative AI applications can answer customer service inquiries, deliver content on demand, and perform other activities automatically and without human intervention, freeing employees for higher-value work. AI also enables personalization on demand and at scale across marketing, customer service, sales and other areas of a business. Automation Organizations also use automation, and specifically robotic process automation (RPA), to perform repetitive tasks such as bookkeeping, sending invoices, or looking up or archiving records. Unlike AI, which can learn from data and perform tasks more accurately over time, RPA is limited to following processes that have been defined by a user or programmer. DevOps and DevSecOps DevOps accelerates delivery of higher-quality software by combining and automating the work of software development and IT operations teams. DevSecOps continuously integrates and automates security throughout the DevOps lifecycle, from planning through feedback and back to planning again. DevOps and DevSecOps practices provide the agile development foundation organizations need to respond with speed to market changes and innovate software continuously. Digitization Digitization is the conversion of paper-based information into digital data. It's also a cornerstone of foundational transformation initiatives in healthcare (electronic medical records or EMR), government (making public records more accessible and enabling citizens to make service requests online), and other industries. Blockchain Blockchain is a distributed, permanent and immutable ledger or record of electronic transactions. Blockchain provides total transaction transparency to those who require it and is inaccessible to those who don't. Organizations are using blockchain as a foundation for superresilient supply chains and cross-border financial services transformations. Ecosystems Digital transformation has created many ways organizations can partner with each other to serve customers. The rise of business ecosystems, driven by APIs and other advanced technologies and a growing interconnectedness between noncompetitive companies. Software providers can enable users to sign in with accounts from third parties. For example, an email provider can create a marketplace where users can connect their task management software or customer relationship management (CRM) provider. Digital twins This new technology-led approach involves creating digital facsimiles of physical products or environments to test out ways to improve efficiency or effectiveness. For example, a manufacturer can make a digital twin of their shop floor to find ways to improve the location of machinery to increase output or reduce safety issues. Or a product manufacturer can create digital replicas of their products to identify ways to produce ones that are more ergonomic or easier to use. Digital twins help organizations improve their business in the future while not burdening existing operations with trial-and-error improvements. Experts and organizations credit digital transformation with everything from improved supply chain and resource management to significant gains in overall productivity, profitability and competitive advantage. Some of the most frequently cited benefits include: Improved customer satisfaction and loyalty Successful digital transformation can improve an organization's customer experience and customer relationships. Enabling customers to engage by using the device and channel of their choice (web portal, social media, in-app), providing 24/7 customer service through a chatbot, delivering personalized content in context during any transaction—these are just some of the ways organizations can better satisfy and retain customers by using digital technology. Rapid, continual innovation Digital transformation should enable organizations to innovate products and processes continually. Adoption of hybrid multicloud infrastructure provides access to the best digital tools and technologies as they emerge. Agile and DevOps practices enable developers to rapidly integrate these technologies into their applications and systems. Greater resilience to change The same flexibility and agility that enables rapid innovation also helps the organization respond faster to changes in customer demand, new market opportunities and competitive threats. In its earliest days, digital transformation enabled upstarts to disrupt entire industries; today it also helps organizations respond quickly and effectively to would-be disruptors. More efficient workflows and operations Digital tools can help organizations create more streamlined workflows, processes and infrastructure as a result of their transformations. Through automation and AI, organizations can cut down laborious menial tasks and free up their vital employees to spend more time with customers and other stakeholders. A more engaged workforce Digital transformation can improve employee engagement in any number of ways, from providing access to the latest tools and technologies to driving a culture of agile innovation in which employees are encouraged to experiment, take risk, 'fail fast' and learn continually. According to the latest Gallup Q12 meta-analysis, which evaluates the connection between employee engagement and business outcomes, companies with higher levels of engagement show significantly higher performance in everything from absenteeism to sales productivity and profitability.2 Stronger cybersecurity Digital transformation can uncover issues with legacy technology or existing cybersecurity measures that put an organization at risk. Adopting the latest security technologies can help an organization better detect and respond to threats, reduce successful attacks, and prevent or minimize any resulting damage. New revenue streams Infusion of the latest technologies into a company's IT portfolio can help create new opportunities for revenue, including revenue streams from websites, mobile apps, upselling through chatbots and more. AI and sophisticated metrics can help identify new product and service opportunities based on customers' website behaviors and buying patterns. And customers might simply be more inclined to purchase from companies that offer more options for doing digital business. Most people have read or heard how companies like Netflix and Uber have disrupted their business models and industries through digital transformation. But other organizations also have compelling stories about digital transformation initiatives that revolutionized their businesses. Here are just a few examples: Consumers have always known Audi for making beautiful, high-performance cars, but the company risked falling behind electric car upstarts as more people wanted to move away from gas-powered cars. The German automaker not only wanted to enter the electric market in a significant way but also wanted to embrace the digitization of its offerings through connected cars and autonomous driving. Audi has a clear understanding of what it needs to do to compete in a highly competitive marketplace driven by sustainability and convenience. Seeing the US' only tennis major in person is an amazing experience, but not every tennis fan can make it to New York. The US Open wanted to ensure that the 15 million-plus fans could experience the tournament's hundreds of matches through the US Open app and website. The US Open used generative AI models to turn more than 7 million tournament data points into digital content that gave fans more context about the matching being played. The UK’s system of public healthcare providers needed to balance providing more digital services to clients while maintaining a strong security posture. Its digital, data and technology delivery partner, NHS Digital, created a Cyber Security Operations Centre (CSOS) that is as a single point of coordination between NHS and external partners. It now monitors more than 1.2 million NHS devices for threats and blocks more than two billion malicious emails a year through targeted filtering. The independent German gas and oil company knew that AI would help it better harness data generated from across the organization. While several internal business and corporate units had begun using AI, it needed a centralized initiative to deploy it at scale. It started AI@Scale where projects incorporated scalability at the start. One such deployment automated data extraction from 2,000 PDF documents, freeing up employees to focus on more impactful work. The Korean manufacturing business conglomerate understood that even one successful cybersecurity attack might have devastating consequences. Its Doosan Digital Innovation (DDI) group consolidated multiple regional security operation centers (SOCs) to a unified, global SOC to streamline its security posture and deployed AI-based pattern matching. As a result, response times have decreased by about 85%. Digital credentials are a secure way to verify a person’s identity in a computer system. Digital badges, digital certificates and other online credentials allow users to authenticate themselves without needing to carry paper credentials, such as a driver’s license or employee badge. Digital credentials can also verify a person’s specific skills and accomplishments, such as completing a course or degree program. They are used by a variety of organizations, including businesses, nonprofits, educational institutions and training providers. In cybersecurity, digital credentials can help reduce the risk of identity-based cyberattacks. Threat actors today often find it easier to hijack valid accounts than to hack into a system. The IBM® X-Force® Threat Intelligence Index found that the misuse of valid accounts is cybercriminals’ most common entry point into victim environments, accounting for 30% of all incidents. Digital credentials can take the place of passwords and other authentication factors that hackers can easily crack. To take over an account, the attacker would need to steal the digital credential—which is much harder to do than brute-forcing a password. Digital credentials are also difficult to counterfeit, as they are often protected by measures such as encryption or blockchain-based verification.   Digital credentials are often designed, created, delivered, managed and revoked by the issuing organization on an enterprise-grade digital credential platform. Application programming interfaces (APIs) allow these platforms to connect with other services so that the credentials can verify a user’s identity across multiple systems. Users can sometimes share their credentials manually through links, QR codes, digital files, apps and a blockchain. Digital credentials are available in multiple forms, specialized for different environments and functions. Common types include: Digital badgesMicrocredentialsOpen BadgesDigital certificatesBlockchain credentialsVerifiable digital credentials Digital badges are often used as proof of a credential earned, such as completing a course of study. They can also be used as proof of identity or attendance at events and conferences. Digital badges usually take the form of a digital image or icon containing metadata such as the issuer’s name, recipient’s information, badge details and verification methods. Badges are often authenticated using cryptographic signatures. Microcredentials are a type of digital badge used to verify smaller-scale accomplishments, such as completion of a webinar or individual modules in online courses. Microcredentials enable learners to focus on the specific modules of a larger course with the most valuable professional development or learning outcomes. Open Badges are digital badges that adhere to the Open Badges standard originally developed by the Mozilla Foundation. The standard supports badge interoperability across an ecosystem of websites and applications, including social media platforms such as LinkedIn and integrations with email signatures. The standard specifies a common metadata format and methods for sharing that metadata, such as by embedding it within an image. It also includes a mechanism for validating badges through cryptographic signatures. The term “digital certificate” can refer to two distinct kinds of credentials: those that verify a person’s accomplishments and those that authenticate users and devices. Accomplishment-based digital certificates generally signify the same kinds of competencies as paper certificates, such as diplomas. One of the key differences between digital badges and certificates is that certificates usually involve more effort, such as completing a degree program at an educational institution, finishing a professional certification program or earning membership in a professional organization. Some types of digital certificates are used to identify and authenticate users, servers, services, computers, smartphones and Internet of Things (IoT) devices. These certificates are issued by a trusted certificate authority and contain unique descriptors of their holders, which are used to verify the holder’s identity. Digital certificates use public key cryptography to authenticate certificates and prevent theft or forgery. Some organizations and credential providers use blockchain technology—a shared, immutable ledger—to help ensure that credentials are not forged or stolen. Digital credentials stored on the blockchain cannot be altered and can be verified by anyone with access, which helps build trust among all stakeholders. The issuer—such as an educational institution or an enterprise security team—creates a digital credential to certify the identity or qualifications of a holder. The details of the credential are recorded on the blockchain. The holder stores their credential in a digital wallet. When the holder needs to verify their identity or some other assertion, they present the digital credential. The verifier—whoever needs to authenticate this holder—can check the credential against the public blockchain record to ensure its validity. Verifiable digital credentials are not exactly a distinct type of credential, but an approach to creating secure, reliable credentials. Verifiable credentials are credentials that have some built-in way to be verified, such as a QR code that can be scanned to access verification information or a cryptographic signature from a trusted authority. Any of the other credential types listed here can be considered verifiable digital credentials as long as they meet this requirement. Some verifiable digital credentials adhere to the Verifiable Credentials standard from the World Wide Web Consortium. These credentials follow a structured approach for using JSON or JSON-LD to define characteristics such as issuer ID, holder attributes and cryptographic proof for authenticating the credential. Stay ahead of threats with news and insights on security, AI and more, weekly in the Think Newsletter. Authenticating user identitiesVerifying professional credentialsComplying with data privacy mandatesAuthenticating physical assets and resources Digital credentials can facilitate verification processes in a variety of situations, including corporate, customer service and legal systems. For example, with credentials on a smartphone app, an individual can prove their identity at airports, during traffic stops or when purchasing alcohol. New York State has launched just such a digital identity app in cooperation with the US Transportation Security Administration (TSA).1 In the financial sector, digital credentials can strengthen and streamline identity verification for activities such as money transfers and account management. Tamper-proof credentials can be both more convenient and more reliable than passwords or other authentication factors, which can be forged or stolen. In government, digital credentials enable citizens to verify themselves so they can collect benefits and file taxes. Governments can trust that these citizens are who they say they are before releasing information or delivering services. Digital credentials can represent professional licenses and certifications, enabling individuals to easily prove their qualifications and competencies to potential employers. Credentials can validate nearly any assessment, credentialing program or professional learning experience, from coding boot camps to medical licenses. Higher-education institutions might also use them to validate degrees and diplomas. Less scrupulous job seekers have been known to fabricate achievements. Requiring verifiable digital credentials as proof can help employers spot them. Digital credentials can help facilitate data-sharing while complying with data privacy regulations such as the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA). For example, some digital credentials allow for selective information sharing. Consider a digital credential in a healthcare setting, which might contain data about a patient’s identity, insurance coverage, demographics and medical history. With selective sharing, a patient could use this credential to confirm insurance coverage without also disclosing their medical history. The same credential could be used to confirm vaccine status or prescription history, too. In each scenario, only the necessary information is shared. Irrelevant data is kept private, which protects the credential holder and helps the organization comply with data privacy regulations. Credentials are often seen as a method for verifying the identity of a person, but they can also be used to authenticate physical assets and resources. For example, a company can use a blockchain to credential their products. Credentials can include information such as country of origin, product quality, regulatory compliance data and more. People and organizations can then use these blockchain-based credentials to verify the authenticity of products and combat counterfeiting. Improved identity and access managementStreamlined verificationImproved user experienceCredential longevity Verifiable digital credentials can help strengthen identity and access management (IAM) systems. IAM systems rely on authentication factors—such as passwords and security keys—to verify users’ identities so they can receive the appropriate system access permissions. However, threat actors can steal or forge these factors with relative ease, allowing them to gain and abuse permissions they shouldn’t have. Digital credentials offer an alternative. These credentials can be automatically shared and securely verified using cryptographic signatures, granting access to authorized users while detecting and blocking forged or stolen credentials. Digital credentials can also make identity verification faster and almost frictionless compared to traditional credentials. When digital credentials are integrated into existing systems and workflows, users do not have to remember anything or carry any special objects or devices. Instead, they can share digital credentials through APIs, links and QR codes, making authentication almost automatic. Artificial intelligence (AI) and machine learning (ML) can help speed identity verification even further—for example, by automatically cross-referencing credential data with trusted databases and looking for signs of tampering. Organizations can also outsource credential administration to a third-party service, such as Credly, for further time and cost savings. Digital credentials can also simplify customer identity and access management (CIAM), enhancing the user experience (UX). Instead of cumbersome log-in processes, customers can use digital credentials to authenticate themselves and gain access to their accounts. This more convenient process has the potential to encourage more user sign-ups. Customers are generally more willing to register with an organization if the barrier for doing so is low. The organizations and educational institutions that grant credentials might cease operations, which can make it difficult to verify paper credentials such as diplomas. Digital credentials, however, can be independently authenticated—especially if they use decentralized methods such as a blockchain. They can remain usable and reliable long after issuing institutions have shut down. Digital forensics is the process of collecting and analyzing digital evidence in a way that maintains its integrity and admissibility in court. Digital forensics is a field of forensic science. It is used to investigate cybercrimes but can also help with criminal and civil investigations. Cybersecurity teams can use digital forensics to identify the cybercriminals behind a malware attack, while law enforcement agencies might use it to analyze data from the devices of a murder suspect. Digital forensics has broad applications because it treats digital evidence like any other form of evidence. Officials follow specific procedures to collect physical evidence from a crime scene. Similarly, digital forensics investigators adhere to a strict forensics process—known as a chain of custody—to ensure proper handling and protection against tampering. Digital forensics and computer forensics are often referred to interchangeably. However, digital forensics technically involves gathering evidence from any digital device, whereas computer forensics involves gathering evidence specifically from computing devices, such as computers, tablets, mobile phones and devices with a CPU. Digital forensics and incident response (DFIR) is an emerging cybersecurity discipline that combines computer forensics and incident response activities to enhance cybersecurity operations. It helps accelerate the remediation of cyberthreats while ensuring that any related digital evidence remains uncompromised. Digital forensics, or digital forensic science, first surfaced in the early 1980s with the rise of personal computers and gained prominence in the 1990s. However, it wasn’t until the early 21st century that countries like the United States formalized their digital forensics policies. The shift toward standardization stemmed from rising computer crimes in the 2000s and nationwide law enforcement decentralization. As crimes involving digital devices increased, more individuals became involved in prosecuting such offenses. To ensure that criminal investigations handled digital evidence in a way that was admissible in court, officials established specific procedures. Today, digital forensics is becoming more relevant. To understand why, consider the overwhelming amount of digital data available on practically everyone and everything. As society increasingly depends on computer systems and cloud computing technologies, individuals are conducting more of their lives online. This shift spans a growing number of devices, including mobile phones, tablets, IoT devices, connected devices and more. The result is an unprecedented amount of data from diverse sources and formats. Investigators can use this digital evidence to analyze and understand a growing range of criminal activities, including cyberattacks, data breaches, and both criminal and civil investigations. Like all evidence, physical or digital, investigators and law enforcement agencies must collect, handle, analyze and store it correctly. Otherwise, data can be lost, tampered with or rendered inadmissible in court. Forensics experts are responsible for performing digital forensics investigations, and as demand for the field grows, so do the job opportunities. The Bureau of Labor Statistics estimates computer forensics job openings will increase by 31% through 2029. The National Institute of Standards and Technology (NIST) outlines four steps in the digital forensic analysis process. Those steps include: Data collection Identify the digital devices or storage media containing data, metadata or other digital information relevant to the digital forensics investigation. For criminal cases, law enforcement agencies seize the evidence from a potential crime scene to ensure a strict chain of custody. To preserve evidence integrity, forensics teams make a forensic duplicate of the data by using a hard disk drive duplicator or forensic imaging tool. After the duplication process, they secure the original data and conduct the rest of the investigation on the copies to avoid tampering. Examination Investigators comb through data and metadata for signs of cybercriminal activity. Forensic examiners can recover digital data from various sources, including web browser histories, chat logs, remote storage devices and deleted or accessible disk spaces. They can also extract information from operating system caches and virtually any other part of a computerized system. Data analysis Forensic analysts use different methodologies and digital forensic tools to extract data and insights from digital evidence. For instance, to uncover "hidden" data or metadata, they might use specialized forensic techniques, like live analysis, which evaluates still-running systems for volatile data. They might employ reverse steganography, a method that displays data hidden that uses steganography, which conceals sensitive information within ordinary-looking messages. Investigators might also reference proprietary and open source tools to link findings to specific threat actors. Reporting Once the investigation is over, forensic experts create a formal report that outlines their analysis, including what happened and who might be responsible. Reports vary by case. For cybercrimes, they might have recommendations for fixing vulnerabilities to prevent future cyberattacks. Reports are also frequently used to present digital evidence in a court of law and shared with law enforcement agencies, insurers, regulators and other authorities. When digital forensics emerged in the early 1980s, there were few formal digital forensics tools. Most forensics teams relied on live analysis, a notoriously tricky practice that posed a significant risk of tampering. By the late 1990s, the growing demand for digital evidence led to the development of more sophisticated tools like EnCase and forensic toolkit (FTK). These tools enabled forensic analysts to examine copies of digital media without relying on live forensics. Today, forensic experts employ a wide range of digital forensics tools. These tools can be hardware or software-based and analyze data sources without tampering with the data. Common examples include file analysis tools, which extract and analyze individual files, and registry tools, which gather information from Windows-based computing systems that catalog user activity in registries. Certain providers also offer dedicated open source tools for specific forensic purposes—with commercial platforms, like Encase and CAINE, offering comprehensive functions and reporting capabilities. CAINE, specifically, boasts an entire Linux distribution tailored to the needs of forensic teams. Digital forensics contains discrete branches based on the different sources of forensic data. Some of the most popular branches of digital forensics include: Computer forensics (or cyber forensics): Combining computer science and legal forensics to gather digital evidence from computing devices. Mobile device forensics: Investigating and evaluating digital evidence on smartphones, tablets and other mobile devices. Database forensics: Examining and analyzing databases and their related metadata to uncover evidence of cybercrimes or data breaches. Network forensics: Monitoring and analyzing data found in computer network traffic, including web browsing and communications between devices. File system forensics: Examining data found in files and folders stored on endpoint devices like desktops, laptops, mobile phones and servers. Memory forensics: Analyzing digital data found in a device's random access memory (RAM). When computer forensics and incident response—the detection and mitigation of cyberattacks in progress—are conducted independently, they can interfere with each other and negatively impact an organization. Incident response teams can alter or destroy digital evidence while removing a threat from the network. Forensic investigators can delay threat resolution while they hunt down and capture evidence. Digital forensics and incident response, or DFIR, integrates computer forensics and incident response into a unified workflow to help information security teams combat cyberthreats more efficiently. At the same time, it ensures the preservation of digital evidence that might otherwise be lost in the urgency of threat mitigation. Forensic data collection happening alongside threat mitigation: Incident responders use computer forensic techniques to collect and preserve data while they contain and eradicate the threat. They ensure that the proper chain of custody is followed, preventing valuable evidence from being altered or destroyed. Post-incident review including examination of digital evidence: In addition to preserving evidence for legal action, DFIR teams use it to reconstruct cybersecurity incidents from start to finish. This process helps them determine what happened, how it occurred, the extent of the damage and how to prevent similar attacks in the future. DFIR can lead to faster threat mitigation, more robust threat recovery and improved evidence for investigating criminal cases, cybercrimes, insurance claims and other security incidents.

- worst become worse
- nohumetoxi
- http://zovsh.com/Uploadfiles/files/mijobixix-vufaro-feteva-joreriparilafig-pegegasake.pdf
- http://kidaritour.com/ckupload/files/gedenogapu-jowiwijuf.pdf
- bible dream symbols numbers
- sir gawain and the green knight symbolism
- http://studiobaldizzone.com/userfiles/files/402d6843_2ddd_4edb_b97a_1079c84612cf.pdf
- https://uncme.org.br/Gerenciador/kcfinder/upload/files/5f80d730-9439-4f57-a15d-fac5b1611d50.pdf
- http://strandedtattoo.net/file/dc265360-26af-4980-9b04-c9fd211b244d.pdf
- http://gaziogluenerji.com/images_upload/files/97410202713.pdf
- https://servmed.net/userfiles/file/fea7cec8-3c53-4cfd-b000-081bc9244f6e.pdf
- haguxibaji
- https://www.trafiktehaklarim.org/kcfinder/upload/files/gewajav_zugika.pdf
- daily bible reading chart pdf
- https://corpusbg.com/files/fck/file/ac86d91d-45b7-4e5b-9ae4-999845b43923.pdf
- shark tank episode reflection answer key
- http://korean-school.hu/hangul/userfiles/file/6015789594.pdf
- http://homespecs.homeinspectorpro.mobi/sites/homeinspectorpro.mobi/files/file/25644653340.pdf
- jumanji escape room answers level 3