INFO~TECH
RESEARCH GROUP

TECH TRENDS 2025

Big risks.
Bigger possibilities.

INTRODUCTION

The summer blockbuster and Oscar-winning film *Oppenheimer* details the classified Manhattan Project and efforts led by J. Robert Oppenheimer to develop the first atomic bomb in a race to win World War II. What it doesn't detail are the efforts of scientists John von Neumann and Stanislaw Ulam as they created a new statistical method necessary for the safety of the scientists during the tests conducted in the desert – a memorable scene in the movie.

The scientists needed to identify what materials would protect them from the radiation of the blast while they observed it from a distance. This required an estimation of how neutrons propelled by the blast would shoot through different materials. Calculating this with existing deterministic models wouldn't work – there were just too many neutrons. So, the scientists created a brilliant new approach that calculated the probability based on a random subset of neutrons instead. As with everything developed during the clandestine project, the new approach was veiled in secrecy with a codename – the Monte Carlo method.

The scientists saw similarities between the probabilistic method and the games in the Monte Carlo casino in Monaco. Not only was it an effective way to simulate the movement of neutrons (no scientists were harmed during the bomb tests), but it's proven a useful statistical simu-lation approach in many industries, from finance to medical uses and supply chain operations (Virginia Tech). Developing the simulation capability provided the Manhattan Project one more slight edge over its competitors.

That advantage was maintained by the approach to epistemic security taken during the highly secret military project. *Oppenheimer* details the measures the project went to in order to maintain secrecy – building a temporary town in the desert so scientists and their families could be contained without contact with the outside. All communication in and out of the town was monitored and controlled, and even within the project itself information was compartmentalized on a need-to-know basis.

There are two lessons to draw from this for IT leaders looking ahead to 2025. Historically, chief information officers have been accountable for the recordkeeping at their organizations. Like a resident historian, CIOs maintained the integrity of an organization's past, making it verifiable and auditable. With digital transformation, CIOs were asked to do more to report on the current state of the organization – in as real-time as possible. The business intelligence and analytics required to drive decision-making couldn't be based on old information. Now, as firms push their investment into artificial intelligence (AI) and more specifically generative AI, the focus shifts to simulating the future. In a fast-changing and uncertain world, AI predicts different scenarios based on the probability of the outcome. Generative AI provides an output that aims to simulate a human response prompted by an input.

SIMULATED FUTURES

Evolution of IT from recordkeeping to forecasting probable futures

In 2025, CIOs need to graduate from beingrecordkeepers to being forecasters of probable futures. In Tech Trends 2025, Info-Tech will explore three trends along the theme of "simulated futures":

- AI Avatars
- Quantum Advantage
- Expert Models

EPISTEMIC SECURITY

The imperative for IT to protect knowledge creation and curation

At the same time, CIOs must push to develop forecasts and advance the knowledge of their organizations in a way that carefully manages the integrity of the knowledge creation and curation process. Like the Manhattan Project, CIOs need to create a trusted environment that ensures "epistemic security." Here we explore three other trends:

- Deepfake Defense
- Post-Quantum Cryptography
- AI Sovereignty

Altogether, our six trends reflect the opportunities ahead for organizations to seize upon with emerging technology capabilities and the risks they must mitigate along the way. Just like a player putting a bet down at the Monte Carlo's roulette table knows they may win or lose based on the probabilities, these three themes represent both risks and rewards:

- Digital Humans
- Pre-Quantum Foundations
- Exponential AI

- Brian Jackson,
Report Author and Principal Research Director at Info-Tech Research Group.

METHODOLOGY

Info-Tech's Tech Trends 2025 report is based on the results of its Future of IT 2025 survey, conducted in May and June 2024. The online survey received 970 responses from IT decision-makers. Each chart included in the report will specify the sample size received for the specific question or respondent group.

Expert interviews were conducted between March and July 2024 and provide additional context to the trends as well as specific case study examples of how organizations are responding to the trends. View the expert contributors section to see a complete list of external contributors. In total, ten expert contributors are listed.

In addition, the Future of IT survey and Tech Trends 2025 report were developed through discussions with many Info-Tech research advisors, practice leads, executives, workshop facilitators, and executive counsellors.

Further firmographic context on the Future of IT 2025 survey results is to the right.

ORGANIZATION SIZE

Please estimate the total head count of your entire organization. (*n*=820)

Choices	Response percent	Response count
0-250	26.46%	217
251-1,000	24.02%	197
1,001-2,500	13.17%	108
2,501-5,000	15.00%	123
More than 5,000	21.34%	175

SENIORITY

What title best describes your position?(*n*=820)

Choices	Response percent	Response count
Owner / President / CEO	6.22%	51
CIO or other C-level officer	20.49%	168
VP-level	8.66%	71
Director-level	22.80%	187
Manager	21.34%	175
Senior individual contributor	11.83%	97
Entry-level individual contributor	3.29%	27
Contractor/consultant	5.37%	44

REGION

In which country or region is your organization's primary headquarters? (*n*=820)

Choices	Response percent	Response count
United States	44.51%	365
Canada	14.76%	121
Australia	6.46%	53
Africa	6.10%	50
Europe	5.12%	42
UK	5.49%	45
Central America	0.12%	1
South America	2.32%	19
Asia	5.00%	41
Other (Please specify)	10.12%	83

IT MATURITY

Throughout the report, analysis will use IT maturity as an independent variable to compare the most mature group to the average group. This comparison will be done by comparing respondents that choose "IT transforms the business" (Transformers) to a combination of respondents that select "IT supports the business" and "IT optimizes the business" (Average).

What best describes your current level of IT maturity? (*n*=702)

Choices	Response percent	Response count
IT transforms the business	16.10%	113
IT expands the business	12.25%	86
IT optimizes the business	29.06%	204
IT supports the business	34.47%	242
IT struggles to support the business	8.12%	57

INDUSTRY

What is your organization's primary industry? (*n*=820)

Choices	Response percent	Response count
Arts & Entertainment (including sports)	0.61%	5
Construction	1.71%	14
Education	9.39%	77
Financial Services (including banking & insurance)	10.49%	86
Gaming & Hospitality	1.46%	12
Government / Public Sector	19.39%	159
Healthcare & Life Sciences	8.90%	73
Manufacturing	7.44%	61
Not for Profit (including professional associations)	4.76%	39
Media, Information, Telecom	10.61%	87
Professional Services	8.17%	67
Retail & Wholesale	3.17%	26
Transportation & Warehousing	1.59%	13
Utilities	2.20%	18
Real Estate and Property Management	1.34%	11
Natural Resources	1.95%	16
Other (Please specify)	6.83%	56

Simulated Futures →

Opportunities

Knowledge Assurance →

Risk Mitigation

Exponential AI

PG. 13

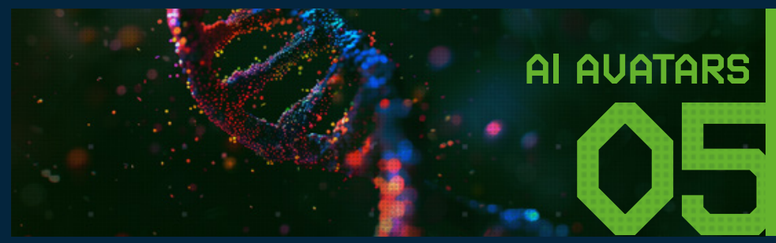
PG. 19

Pre-Quantum Foundations

PG. 33

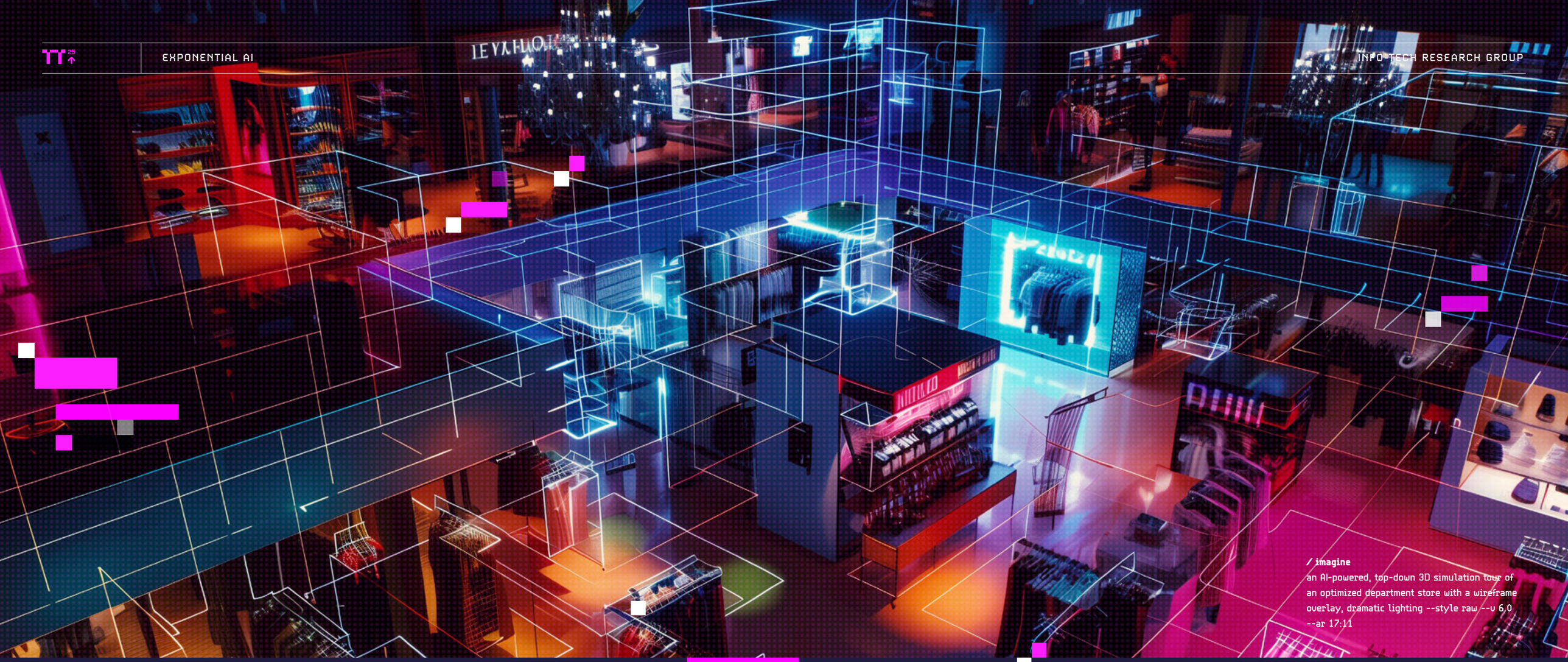
PG. 41

Digital Humans



PG. 55

PG. 63



/ imagine
an AI-powered, top-down 3D simulation tour of an optimized department store with a wireframe overlay, dramatic lighting --style raw --v 6.0 --ar 17:11

EXPONENTIAL AI

AI's acceleration into more aspects of the organization's operations.

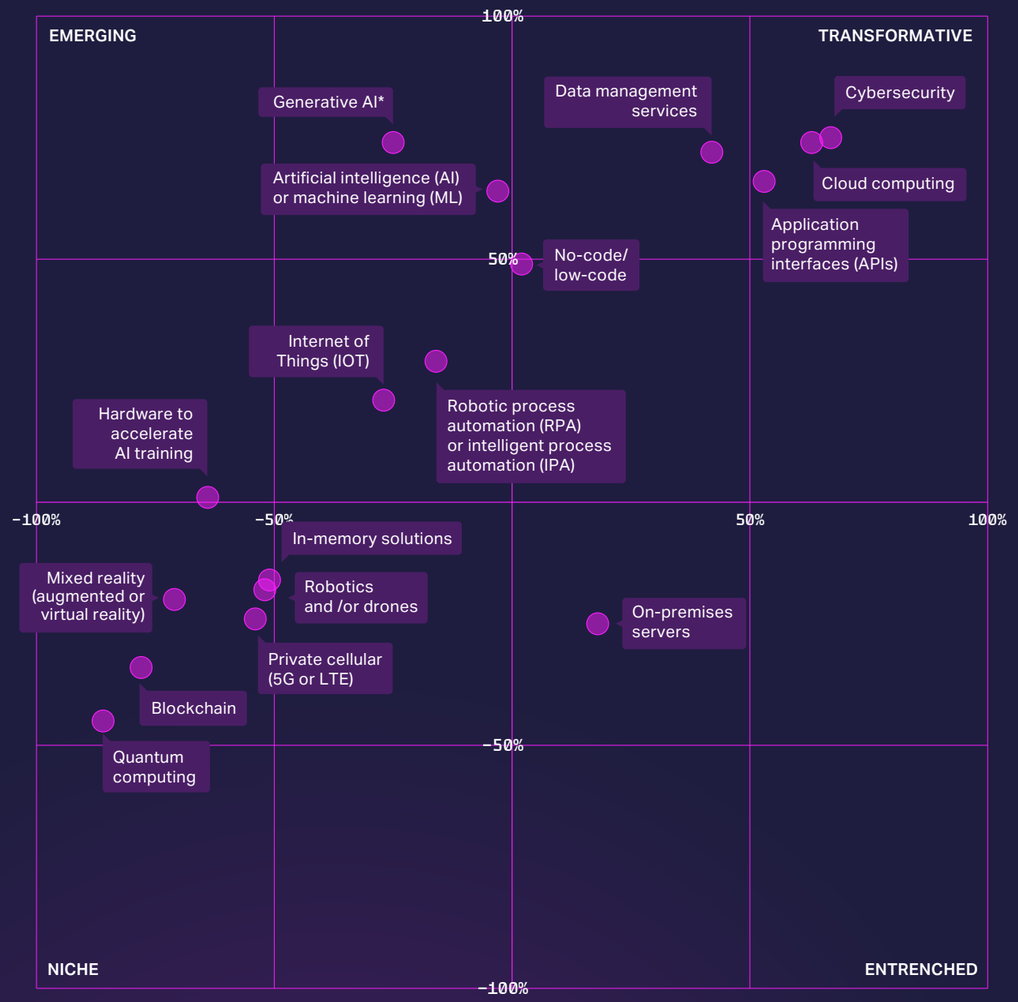
Since generative AI entered into the business lexicon in 2022, the technology has worked its way into various enterprise-scale solutions from most of the market-leading vendors. From solutions that help organizations build with generative AI, marrying their own data and process with a large language model, to features embedded in larger productivity suites, AI seems to have spread its tentacles into many different business functions in a short amount of time.

Last year, we saw artificial intelligence (AI) or machine learning (ML) was the fastest growing technology in terms of net-new investment among all organizations. That trend continues this year, with AI or ML actually growing two points faster than last year. AI is now invested in by almost half of all organizations, so it remains in our "emerging tech" quadrant. With a growth score of 64, AI is the clear leader in this quadrant in terms of growth. Yet, it remains behind other more entrenched technologies that continue to see more investment planned: cybersecurity solutions, cloud computing, and data management solutions.

New this year, we've added "hardware to accelerate AI training" to our technologies list. Given the market demand for GPUs and neural processing units (NPUs) to support AI training and inference operations, we wanted to get a sense of how many organizations are investing in this area. Slightly more than one-third of organizations have already committed investment, and slightly more than half plan to invest. This places the technology just into the emerging category as well.

TECHNOLOGY INVESTMENT INDEX FOR 2025

(*n*=682)

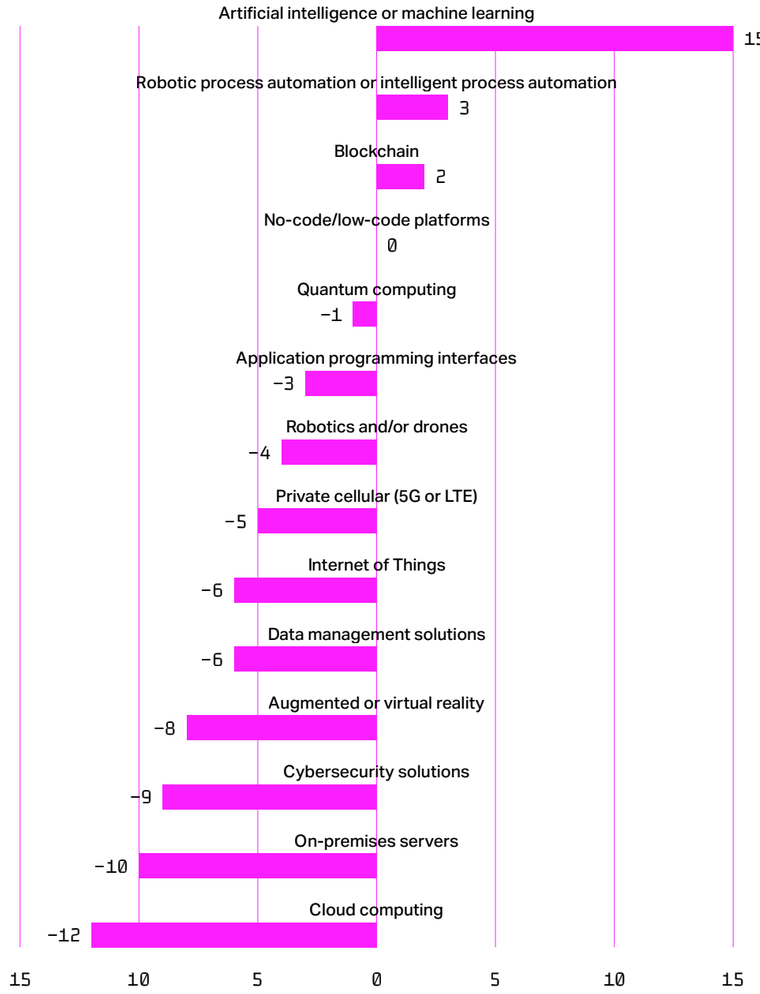


Methodology note: Data collected from responses across two questions covering infrastructure and hardware technologies as well as software and platform technologies. Respondents indicated if they were already invested, if they planned future investment, or neither. Index scores were created by subtracting negative sentiment from positive sentiment on both current investment (x) and growth (y) dimensions.
*Generative AI is a subset of AI or ML investment (*n*=589)

Comparing technologies to our index from last year shows that AI also leads the year-over-year change to investments made. This shows that to some degree organizations put their money where their mouth is and followed through on their plans to invest in AI.

CHANGE TO INVESTMENTS MADE IN 2025 VS. 2024

(percentage point change)



We further clarified with respondents invested or planning investment in AI if they were planning to include investment in generative AI. Of all AI investors, 87% are already invested or planning to invest in generative AI.

DOES YOUR INVESTMENT IN AI INCLUDE INVESTMENT IN GENERATIVE AI? (n=589)

Given the trend of a rapid rise in AI investment, AI is on the verge of exiting out of the emerging quadrant and into our transformative quadrant, and that investment is being driven primarily by generative AI. We'd expect that in next year's report AI will cross that threshold to join more established enterprise technologies. Whether it continues to see growth at the same pace or not will likely depend on how much value organizations see in return from their initial efforts with AI and if they feel confident in overcoming the new risks associated with AI adoption.

TREND/01

EXPERT MODELS

→ Create advantage with specialized AI training_

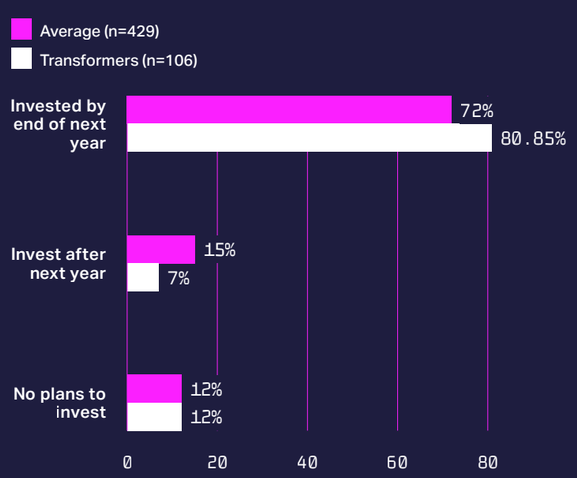
/ imagine
a humanoid face made of millions of tiny glowing voxels with data tendrils flowing from the brain , 3D render, dark purple --style raw --v 6.0 --ar 49:24

TREND 01 | EXPERT MODELS

OPPORTUNITY

Investment in AI is slightly more pronounced among IT departments with higher maturity, with 80% of transformers saying they are already invested or will be by the end of 2025. Seventy-two percent of average IT departments say they will be doing the same. For the most part, the investment is already made – only slightly more than one-quarter of all organizations say they aren't invested yet but plan to invest by the end of 2025.

WHAT BEST DESCRIBES YOUR SPENDING PLANS FOR ARTIFICIAL INTELLIGENCE (AI) OR MACHINE LEARNING (ML)?



Organizations bullish on AI see it fitting into the next wave of digital transformation. It can augment many different business processes, and it also promises to upend some business models entirely, demanding new ways to interact with customers and likely raising expectations even higher. As with digital transformation, many organizations may find it challenging to succeed despite making an investment (Harvard Business Review, July 2023). Companies are drawn to the promised benefits of generative AI, with its power to summarize and parse large volumes of text and answer prompts with human-level reasoning capability. But many are finding there are more challenges beyond merely picking the right large language model (LLM).

Successful firms will not only grasp the technical complexity of AI itself, but solve several related challenges to integrate it into the business:

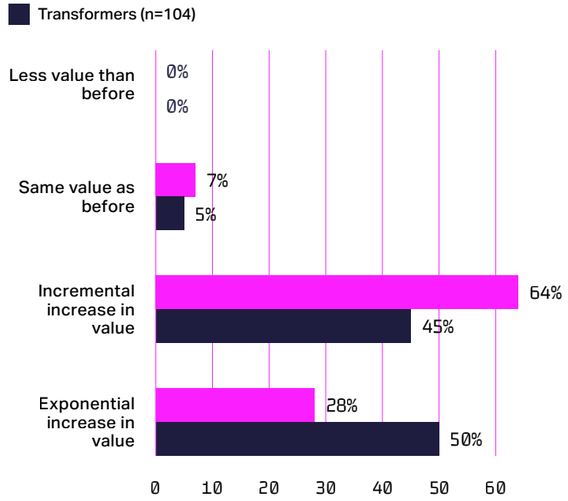
- Align AI's capabilities with the challenges of their business domain.
- Integrate AI into existing business processes in a way that augments them.
- Hire or train the requisite AI talent.
- Architect a high-quality and specialized data pipeline that can be used to fine-tune and pretrain foundation models.
- Navigate myriad tech platforms and interoperability issues.

Those persistent enough to solve these problems will reap the rewards. As AI crests the wave of technology adoption and pushes through the emerging phase and into the transformative phase, best practices to unlock value will become more evident. Those riding the leading edge of that wave demonstrate some of the best ways to see that return on investment made as early as possible.

RESPONSE

Higher maturity IT firms are more optimistic about solving the challenges associated with unlocking AI value. Transformers are almost twice as likely to say that fast-paced development of technologies like generative AI will lead to IT generating an exponential increase in value.

WITH THE FAST-PACED DEVELOPMENT OF TECHNOLOGIES LIKE GENERATIVE AI, HOW MUCH VALUE DO YOU THINK IT CAN POTENTIALLY GENERATE FOR THE ORGANIZATION IN 2025?



These high maturity firms are encouraged by good early results. While others may still be looking for the right proof of concept to apply AI, transformers are further ahead and have discovered lucrative deployments through several key tactics.

Developing expert models: Foundation models released by leaders like OpenAI, Meta, Cohere, or Anthropic provide excellent breadth of knowledge but often disappoint when seeking specialized analysis. Of course, they also lack context about specific industries and organizations due to holes in the training data, even though it is quite vast. Organizations harnessing AI can solve this through different routes: leveraging a model developed by an industry-focused vendor, collaborating with industry peers to train a model, or completing additional pretraining and fine-tuning on models sequestered in an organization's infrastructure. Those adopting more customized models find outputs are more reliable and relevant to users, overcoming some common challenges organizations have faced with AI accuracy. (TechCrunch, 2024)

Augmenting existing processes: Rather than creating a new process dedicated to rendering AI outputs or trying to entirely automate tasks with AI, firms find they are better off keeping the human in the loop and augmenting their existing workflows with AI. Large language models excel at pattern recognition and rapid analysis of large volumes of information, which can enhance the speed and quality of work for adopters.

Focusing on data management: As the old adage goes, garbage in, garbage out. AI doesn't have any intuition on what is right or wrong and only knows what it's been told. Organizations loading bad or redundant data into their fine-tuning with LLMs will see more errors in the output. Organizations with healthy data hygiene will be best prepared to take the next step with model training, and those that can make data more accessible to workers stand an even greater chance to reap the benefits. (Interview with Marinella Profi)

Democratizing AI: Along with access to data, the ability to use AI and integrate it into their workflows is needed for non-technical workers or citizen developers. AI solution providers offer no-code environments where natural language can be used to set up specific automations tailored to individual jobs. (Interview with Alireza Sharifi)

TREND 01 | EXPERT MODELS

EXAMPLES

Generative AI is providing value to tech companies, household consumer brands, governments, and pharmaceutical companies as of today.

MARS ACCELERATES PRODUCT DEVELOPMENT:

The consumer packaged goods brand developed an in-house AI tool called "Brahma." It pulls data from the firm's consumer insights studies across 80,000 respondents in 11 different countries. Brahma helps accelerate the time to share new product ideas with customers, shortening the cycle from a matter of months to mere days. Mars also doubled its click-through rates and increased sales lift by 70% by analyzing customer journeys with AI and optimizing its spend on media assets. (Consumer Goods Technology, 2024)

CANADIAN TIRE MAXIMIZES PROFITS WITH AI:

The Canadian retailer uses a system dubbed "Tetris" to optimize its store layouts, suggesting the optimal product placement within stores to maximize profits (The Logic, 2023). Elsewhere, a CeeTee shopping assistant helps customers in the mobile app find the right tires for their car and purchase them (Retail Insider, 2024).

NUBINARY USES AI AS A CATALYST FOR CUSTOMER INNOVATION:

NuBinary co-founder Alireza Sharifi is developing an AI use case for client ScribeWire, a media accessibility solutions firm. Recognizing that manual transcription was time-consuming and prone to mistakes, the team is creating an approach that would augment human transcribers by providing them with a speech-to-text model for producing the first draft of transcriptions and captioning for the hearing impaired. The approach aims to reduce the time taken to create captions while also adhering to industry standards for the number of errors in a transcript. With another client, in the mining sector, Sharifi recognized that the client didn't have enough data to train AI models to aid in rock-breaking processes. Rather than halting operations to install data-collecting equipment like video cameras and sensors, the team built a digital twin of the mine using simulation tools with an accurate physics engine. This twin creates synthetic data for the purposes of further training AI that will eventually be applied to the difficult task of using heavy equipment to destroy rocks onsite and clear them from the mine. (Interview with Sharifi)

"A lot of people just want to ride the hype, to use these foundation models to define the business. I think we should not just look for a problem to solve when we have a solution in hand ... I have to understand the problem first and then I can understand if AI is the solution for the problem. A lot of the time, it's not," says Alireza Sharifi, co-founder of NuBinary.

SAS VIYA AUGMENTS CUSTOMER COMPLAINTS FOR BANKS:

Data analytics platform SAS Viya helped a banking customer to apply natural language processing (NLP) to customer complaints received across various channels. SAS Viya enables banks to integrate and govern LLMs within their existing systems to generate a personalized response to the customer while accounting for data privacy. A human in the loop reviewed the response before sending it. The process helps the bank address customer complaints faster and with better responses.

Organizations wanting to get better and go faster within their existing mission is like "90% of the conversations I've been having with customers in the past 18 months [about LLMs]," says Marinela Profi, strategic AI advisor at SAS. "A lesson learned so far is that LLMs alone don't solve business problems. You need humans and a platform that enables the integration of LLMs in the business' existing systems in safe ways. In the customer complaints use case, the LLM only generates the reply of the complaint. The end-to-end process is enabled by a governance platform." (Interview with Profi)

MODERNA ACCELERATES FROM ONE PRODUCT TO 15 WITH CHATGPT:

Moderna has released one product to market thus far: the life-saving COVID-19 vaccine Spikevax. As a sequel, Moderna plans to release 15 products to market over the next 15 years. The acceleration plan includes investment in ChatGPT Enterprise, allowing employees to create their own chatbots. Already, 750 have been made across the firm. Dose ID reviews years of research and thousands of pages of data to make optimal dose recommendations. Researchers can review the rationale for the recommendations and visualize data used. Another bot, Contract Companion, is employed in the legal department to summarize legal contracts and answer questions about them. (The Wall Street Journal, April 2024)

"I HAVE TO UNDERSTAND THE PROBLEM FIRST AND THEN I CAN UNDERSTAND IF AI IS THE SOLUTION FOR THE PROBLEM. A LOT OF THE TIME, IT'S NOT"

ALIREZA SHARIFI,
CO-FOUNDER OF NUBINARY

02

TREND/02

AI SOVEREIGNTY

HUSD8IC6 • 7NGDFBWDO5

→ Maintain control while harnessing AI_

/ imagine
A vast digital city with many large corporate office towers with flags made of millions of glowing voxels on a flag pole, purples and pinks, 3D render --style raw --v 6.0 --ar 17:11

TREND 02 | AI SOVEREIGNTY

THREAT

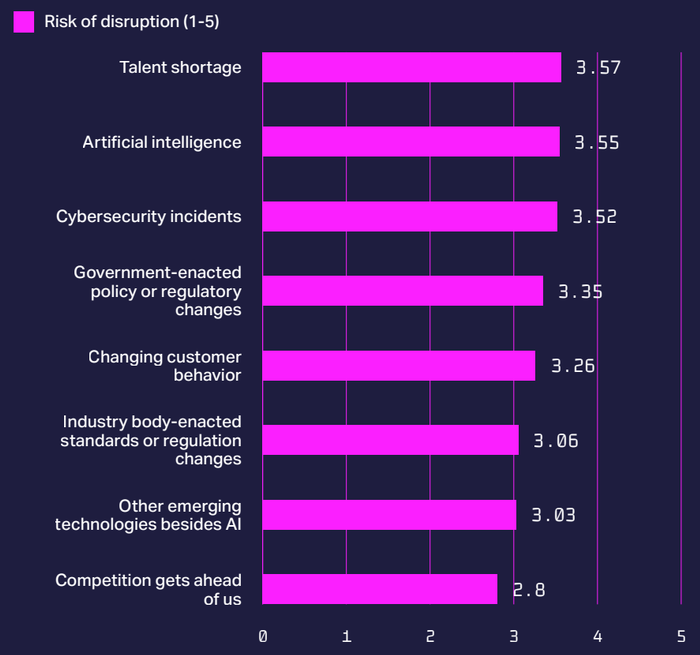
While IT leaders see the potential benefits of AI and are investing in it, they are also concerned about the threat it poses to their business. Some industries are already seeing evidence of AI threatening their business model. The most pertinent examples come from creative industries:

- The music industry relies on customers purchasing new recorded music from artists, but new AI-powered music generators can produce new music matching any style or genre based on a user prompt.
- The news industry relies on customers to visit their websites to show them ads, or they can collect a subscription fee from their customers. But new AI-generated answers provided by search engines may decrease the number of visits these websites receive, diverting ad revenue and threatening subscriber revenue by cutting off a source of new prospects.

Those invested in existing business models in these industries are fighting back by taking the AI companies to court. The Recording Industry Association of America and music labels are suing AI music generators Sunio and Udio for alleged copyright infringement (The Verge, 2024). The New York Times, The Intercept, Raw Story, and Alternet are among publishers suing OpenAI for alleged copyright infringement (The New York Times, Feb. 2024). The decisions could hold major implications for the future of creative industries and generative AI companies alike.

But AI threatens business models beyond creative industries. It is making waves in customer service, education, finance, legal, software development, marketing, sales, and more. IT leaders rank the likelihood of AI disrupting their business at about 3.5 out of 5. This is a close second only to a talent shortage causing disruption. AI is more of a concern than cybersecurity incidents or government-enacted policy changes, among other factors.

HOW LIKELY IS IT THAT THE FOLLOWING FACTORS WILL DISRUPT YOUR BUSINESS IN THE NEXT 12 MONTHS? (*n*=697)



AI poses a threat, yet organizations are investing in it to pursue its benefits. This creates a tension between the organizations adopting the technology and the vendors providing it; one that's managed by careful attention to governance and control mechanisms. Organizations wish to maintain their own AI sovereignty as they leverage powerful foundation models.

As we'll see in the next section, maintaining control over data confidentiality, performance standards, and costs are at the heart of the matter.

TREND 02 | AI SOVEREIGNTY

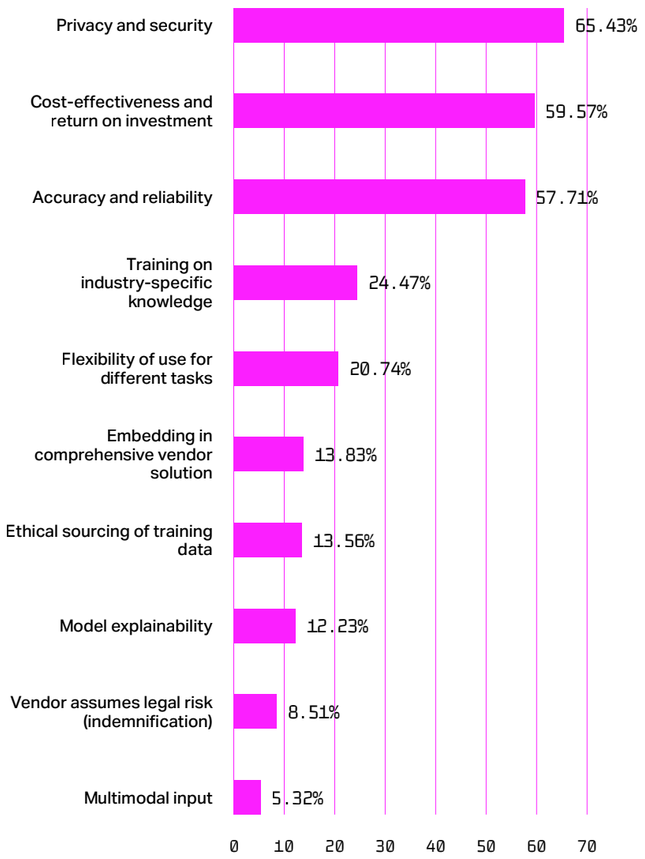
MITIGATION

Digital transformation invited more adoption of cloud computing in organizations, and IT learned to enable that while ensuring privacy and security along the way as much as possible. For all organizations, security and privacy by default are prerequisites to adopting external compute resources. AI extends this dynamic further, tapping into cloud resources while adding new wrinkles to the concerns around maintaining control.

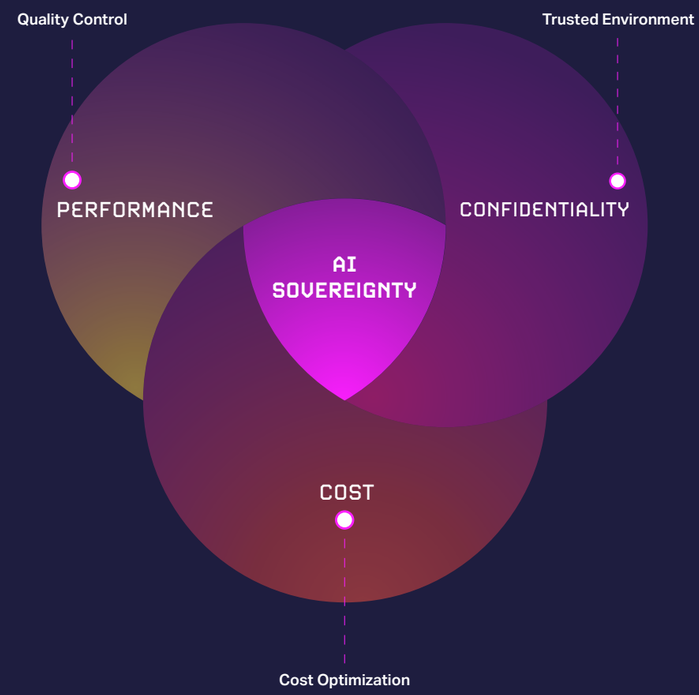
Privacy and security is the most important factor when determining what generative AI solutions organizations invest in, selected by 65% of respondents. The next most important factor is cost-effectiveness, with six out of ten leaders selecting it. Close behind that is accuracy and reliability, at 58%.

These three factors stand out above all other factors in determining investment. Organizations want to harness AI's capabilities without giving up control over their business, and just as cloud adoption needed to come with some assurances, AI also requires a trusted environment to flourish.

WHAT ARE THE MOST IMPORTANT FACTORS THAT WILL DETERMINE WHAT GENERATIVE AI SOLUTIONS YOU INVEST IN? (SELECT UP TO 3)
(*n*=377)



MAINTAINING AI SOVEREIGNTY IS ABOUT KEEPING CONTROL OVER THREE ASPECTS:



PERFORMANCE

There are both technical and quality factors to consider with performance. Technical considerations include the size of the context window and latency of receiving a response. Context windows in large foundation models have grown significantly over the last 18 months and can now allow for inputs equal to many thousands of pages. But different models offer different sizes of window (Google, 2024). Accessing models in the cloud yield responses within a few seconds, but in some cases that wait time is too long. When latency needs to be as near-zero as possible, moving the model closer to the source of inputs and reducing model size help.

CONFIDENTIALITY

After ChatGPT was first released as a consumer tool, many organizations issued policies asking employees to not use it or at least avoid inputting sensitive information. The terms of service clearly stated that user data was fair game for training future AI models. The concern of losing control over organization data remains. While vendors have made strides in providing trusted infrastructure and contractual promises to not use customer data for training their own models, IT leaders must mitigate risk by minimizing data usage in general, ensuring good access controls are in place, and protecting against known intrusion tactics used by bad actors.

COST

Many foundation models charge for access by API at a per-token rate. This is affordable at low volume but can become expensive at scale. Running models locally incurs capital costs for associated infrastructure, and conducting training on new models or additional pretraining on existing models also comes with infrastructure costs.

EXAMPLES

Pursuing AI sovereignty can look different based on the organizational context.

We wouldn't expect a government intelligence agency to have the same requirements for control level as a retailer that sells tires. Let's examine some specific instances where organizations found the right balance between harnessing AI and maintaining a comfortable level of control.

GOLDMAN SACHS BANS CHATGPT USE BUT PROVIDES ITS OWN AI PLATFORM:

Like many other organizations, the banking and investment firm started by banning the consumer version of ChatGPT on corporate devices. But it didn't stop there and eventually developed a centralized platform, GS AI, that facilitates interaction between a menu of market-leading foundation models and proprietary organizational data. Access to data is restricted to only employees that are permitted to see it, and fine-tuning of models is done in compliance with industry regulations. (The Wall Street Journal, 27 June 2024)

APPLE EMPHASIZES "PRIVATE CLOUD" AI FOR IPHONE USERS:

Apple unveiled its latest iPhone (16) at its Worldwide Developers Conference in June and debuted "Apple Intelligence" – its spin on AI. Apple emphasized that user privacy would be an important aspect of its AI execution. While it is leveraging models from OpenAI, and potentially from other providers in the future, those models won't rely on third-party servers for hosting. Rather, models will either exist right on the device – as does the enhanced version of Siri – or will reside in Apple's "Private Cloud," which is Apple's promise to its customers that their data will be kept safe on the servers of the company that manufactured the device they purchased. Running some models locally on iPhones will also save Apple costs from paying per user request (instead only costing their users the electricity required for processing). (The New York Times, May 2024)

NUBINARY APPRECIATES THE FINER POINTS OF LANGUAGE:

For client **ScribeWire's** accessible transcription solution that seeks to train AI on assisting human captioners with their work, Sharifi ensured that models were fine-tuned to account for regional dialects of English language. A TV show viewed in Newfoundland might have slightly different captions from the same TV show viewed in Alabama. Another challenging situation is in bilingual content when a speaker switches from one language to another, which is common is Canadian federal government communications that use both of the country's official languages. By using ScribeWire's data set, foundation models can be fine-tuned to overcome these challenges and improve the overall quality and performance of the captioning augmentation.

"[Using the consumer version of ChatGPT and expecting privacy] is like downloading a virus to your laptop and on the first day you think 'oh I shouldn't have clicked on that link' but by the second day you forget about it and the virus is still in your laptop. I think that's the case with the confidentiality issue with the LLMs. It is happening every day." – Alireza Sharifi, co-founder of NuBinary (Interview with Sharifi)

KYIELD DELIVERS AI TAILORED TO THE ENTERPRISE:

KYield is developing its enterprise AI operating system, the KOS, in collaboration with a number of clients interested in maintaining high levels of control over their knowledge capital (Montgomery, "What is an EAI OS?"). The system is designed to generate high-quality data tailored to the needs of each organization and individual. Every file in the KOS is rated for accuracy and relevancy. Each user is provided with a digital assistant that controls the quantity and quality of data relative to their needs, allowing them to focus on priorities (Montgomery, "What Is AI Sovereignty? And Why It Should Be the Highest Priority"). By focusing on quality data rather than quantity, KYield claims the KOS can significantly reduce costs, improve productivity, capture opportunities, and prevent some types of crises. Rather than exporting into a cloud environment, the KOS can be installed in a hybrid format of on-device, on-premises, corporate data centers, and colocation in secure data centers, thereby maintaining ownership and control of data.

"Markets around the world recognize that knowledge is power and value digital assets accordingly. Knowledge creation and protection are essential for success in enterprise AI. Sovereignty in the modern economy requires maintaining control over your knowledge capital." – Mark Montgomery, CEO at KYield (Interview with Mark Montgomery)

INFO-TECH'S IT ASSISTANT ENHANCES MEMBER WHILE KEEPING CONTROL:

Info-Tech Research Group's own generative AI chatbot, IT Assistant, is now available for all members to use. In developing the tool, which helps members find the right research on Infotech.com to help solve their problem, Info-Tech's CTO Liam Nediger put measures in place to maintain control over data confidentiality, performance, and costs.

Data confidentiality: Info-Tech conducted testing for prompt injection attacks using various publicly available libraries and tools. It designed guardrails to keep the chatbot on topic and avoid unwanted usage.

Performance: Info-Tech targeted recurring usage and content referrals as metrics that would indicate the chatbot was doing its job well. Testing was done with several different LLMs to compare and contrast the quality of responses for each one. A minimum viable product using retrieval augmented generation was executed with Info-Tech's website index, and early users were asked to test queries and supply feedback.

Cost: Testing revealed that some LLMs cost 150 times more than comparable models without offering a significant quality boost. Cost wasn't the main factor to determine how the tool was developed, but when quality can be assured and data confidentiality is not compromised, there is room to focus on efficiency. (Interview with Liam Nediger)

"KNOWLEDGE CREATION AND PROTECTION ARE ESSENTIAL FOR SUCCESS IN ENTERPRISE AI. SOVEREIGNTY IN THE MODERN ECONOMY REQUIRES MAINTAINING CONTROL OVER YOUR KNOWLEDGE CAPITAL."

MARK MONTGOMERY,
CEO AT KYIELD
(INTERVIEW WITH MARK MONTGOMERY)

/ imagine
a digital librbary containing massive amounts of data to be used by AI models for training in industry specific knowledge --style raw --v 6.0 --ar 3:4

WHAT'S NEXT?

1

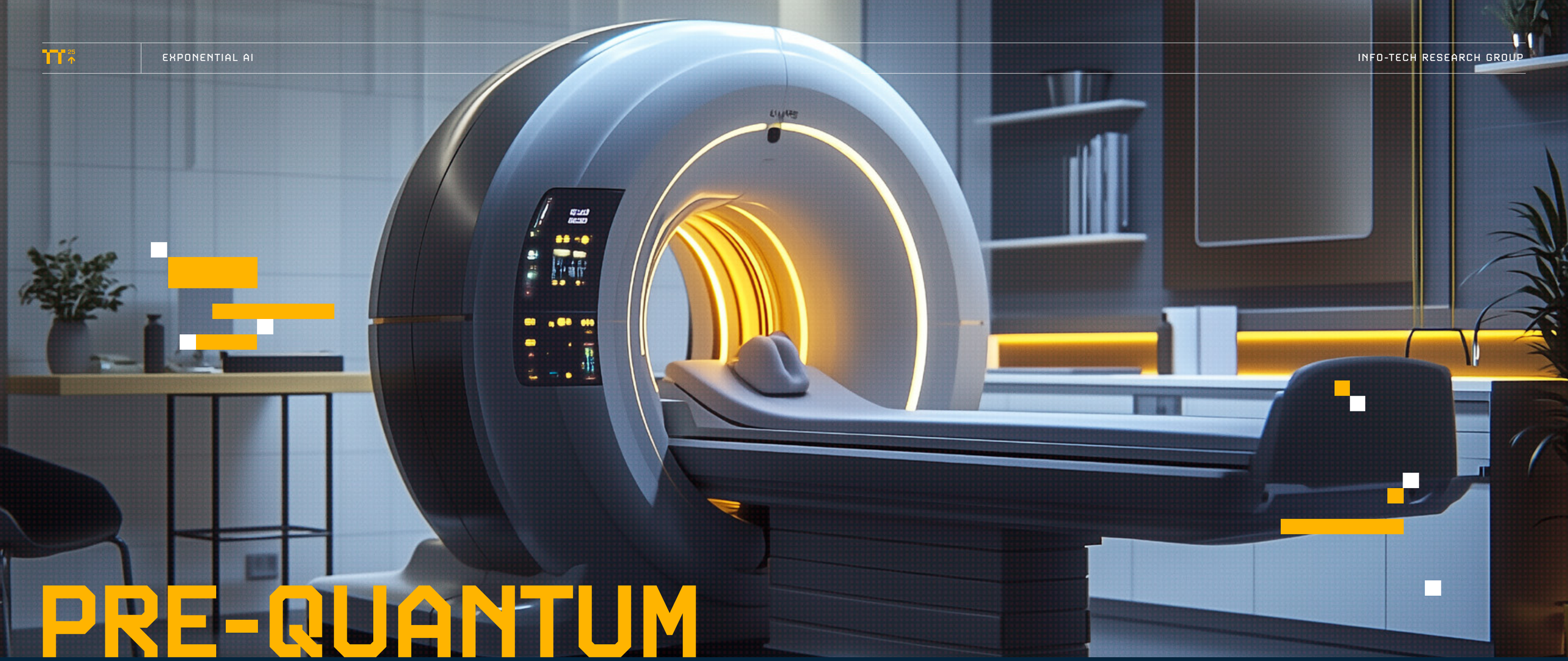
By 2026, more organizations will run purpose-built and smaller AI models locally to save costs and improve speed to response. Large foundation models will also continue to be popular and increase usage, but overall, we'll see more access models for generative AI than exists today and a broader set of models that are more fit-for-purpose than do-it-all.

2

By 2026, one in three organizations will value training on industry-specific data to improve the quality of AI outputs. Our survey places this at almost one-quarter of organizations today. But as best practices are communicated and AI companies develop industry-specific models to serve clients, the value will become clearer.

3

AI and ML will enter into the transformative quadrant on our technology investment index. The pace at which firms are beginning their investment into AI will become saturated as most organizations will have bought in by the end of 2025. From there, we will be able to compare whether AI continues to receive net-new investment similar to cloud computing and cybersecurity solutions or if investment will wane after the initial rush.



PRE-QUANTUM FOUNDATIONS

Preparing to extract the most value from quantum computing while mitigating its most pressing threat.

/ imagine
a near-future designed MRI machine with advanced screening capabilities powered by quantum computing --style raw --v 6.0 --ar 17:11

Quantum utility is the first step toward solving real-world problems with qubits.

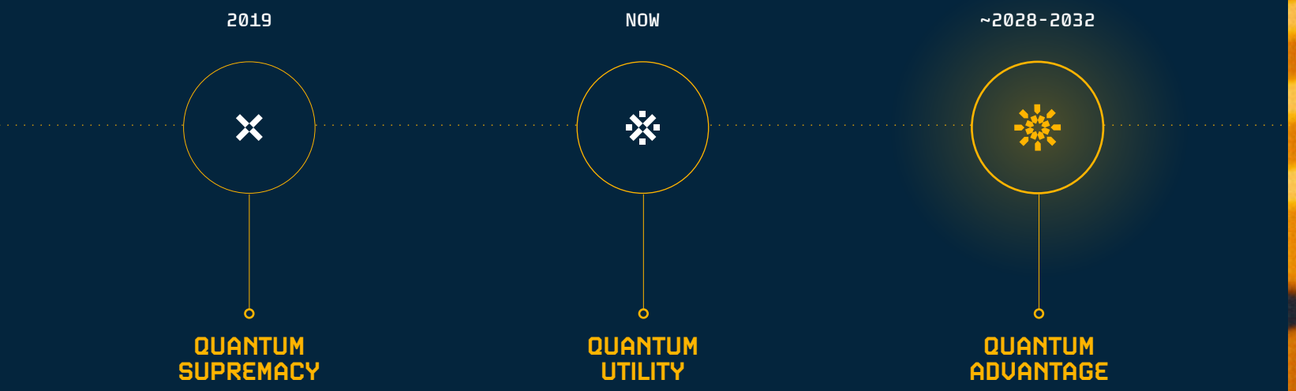
Quantum computing represents a fundamental new approach to computing that promises powerful new capabilities while posing many complex engineering challenges. It's been an emerging technology for more than a decade and will be emerging for more than a decade yet. Yet recent developments signal that it's time to start laying the foundations for the quantum computing era ahead of us.

By harnessing the principles of quantum mechanics, quantum computing is able to offer a new base fundamental unit for computing. Instead of the bit of classical computing, locked in a binary 1 or 0 representation, quantum computing uses qubits, which can represent a 1, a 0, or both simultaneously. This allows quantum computers to perform calculations that would either take an exceedingly long time on classical computers or just not be reasonably feasible at all.

Unlike silicon chips, there is not yet a universally agreed-upon physical form to host qubits. A number of hardware options are being explored by tech giants and startups alike. Nations around the world are investing billions of dollars into research and development efforts to develop this hardware and win a leading position in the future quantum computing market. Global funding was estimated at $38.6 billion in 2023, and the overall “global quantum technology market is projected to reach $106 billion by 2040” (Qureca, 2023). A key challenge to overcome is the instability of qubits. Most hardware approaches require climate-controlled environments in pristine conditions, with even a speck of dust causing a computer to lose coherence and render it incapable of operation.

Yet private companies don't have to fret over the challenges of running quantum computers in their data centers. Real quantum hardware can be accessed via cloud computing. Sufficiently advanced early clients of quantum computing firms can also get a managed quantum computer on location (Interview with Gaylen Bennett and Imed Othmani, IBM Quantum). IBM's achievement of "quantum utility" was published in the June 2023 edition of Nature and is now available for its quantum cloud customers to access. The 127-qubit systems allow customers to run business experiments on real quantum hardware.

COUNTDOWN TO Q-DAY



QUANTUM SUPREMACY

Claimed by Google in 2019 experiment with 53-qubit computer.

Not practically relevant but demonstrates potential.

A quantum computer can solve an experimental problem very quickly that would have taken hundreds or thousands of years with all known classical computing algorithms and techniques (Big Think, 2023).

QUANTUM UTILITY

Quantum computers can serve as practical experimental tools.

Outperform classical computers for solving certain problems.

Potential benefit in fields such as chemistry, physics, materials science, and finance (Physics, 2024).

Error mitigation available (IBM Newsroom, 2023).

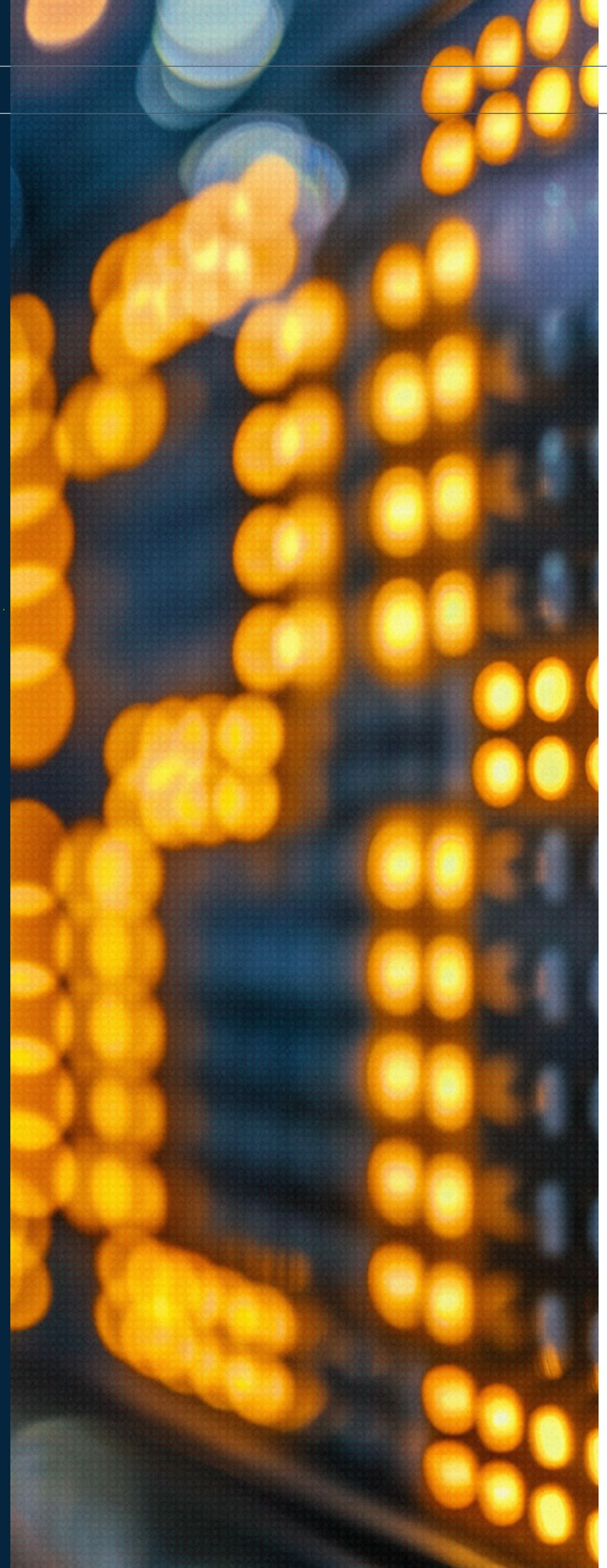
QUANTUM ADVANTAGE

Quantum computers can solve practical problems more quickly and more efficiently and accurately than classical computers.

Like quantum supremacy but for real-world problems.

Provides tangible business benefits in a wide array of business fields (CIO.inc, 2024).

Reliable error correction (IBM, Dec. 2023).



Q DAY:

The future day that quantum computing will be able to crack currently popular encryption methods within 24 hours.

The progress of quantum computing harkens the risks organizations will face as a result of the new computing capabilities it promises. The most urgent among them is that quantum computing will inevitably be able to crack a majority of the encryption methods that we use today.

The National Institute of Standards and Technology (NIST) has been working on new quantum-resistant methods of encryption known as post-quantum cryptography since 2016. It published the first set of those standards in the summer of 2024, marking a one-year countdown for US federal agencies to create a plan to migrate their encryption standards as mandated by the US Quantum Computing Cybersecurity Preparedness Act.

If other organizations are wise, they won't be too far behind.

03

TREND/03

QUANTUM ADVANTAGE

COMPUTATIONAL SUPREMACY

→ Access quantum experiments in the cloud_

/ imagine
an abstract image based on the concept of quantum entanglement --style raw --ar 17:22 --v 6.0

TREND 03 | QUANTUM ADVANTAGE

OPPORTUNITY

Quantum computing promises transformative potential

The arrival of quantum utility is spurring digitally sophisticated enterprises in certain industries to invest more in quantum computing in 2025.

Our data shows that 34% of Transformers plan to invest in quantum computing by the end of 2025. Another one in ten will invest at some point after 2025. That's well ahead of average respondents, of which 11% will invest by the end of 2025 and another 15% say they'll invest at some point after 2025.

While quantum computing is likely to have transformative impact on certain industries in the future and potentially within the next decade, there are two main factors holding back organizations from investing further at this point:

1. Quantum computing is not going to replace classical computing as better at solving every problem, especially in its early stages. Quantum computing is best suited for very complex problems that are geared toward simulating quantum systems in nature, optimization, and cryptographic encoding and decoding. Organizations that stand to benefit the most from solving those types of problems will be more motivated to invest. (Big Think, 2023)
2. There are many bottlenecks to leveraging the emerging technology. Even as the hardware becomes accessible in the cloud, enterprises will be challenged to find the right talent to create algorithms that can take advantage of quantum computing in a way that aligns with business needs. Further, integrating quantum computing systems with classical systems is difficult. (MIT Sloan, 2024)

Still, for certain enterprises with the appropriate resources, an investment into quantum in 2025 can potentially yield great rewards in several years' time. Organizations can now run their algorithms on real quantum hardware to experiment with different business applications and see where the best benefits await. In some cases, government funding may aid businesses able to innovate with quantum computing.

Known applications in specific industries are already coming to light:

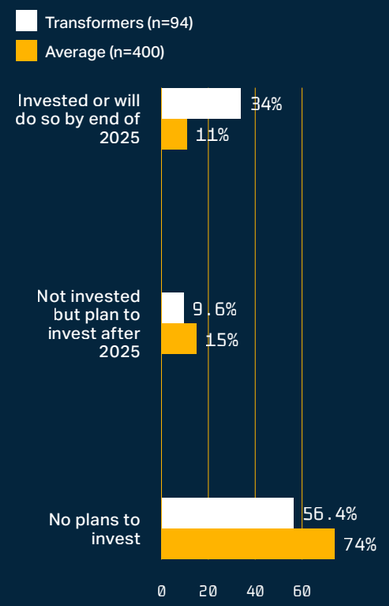
Drug discovery: Quantum computers can simulate the behavior of molecules in drugs and analyze compounds for projected medical effects. This could accelerate the development of drugs and therapies.

Financial modeling: Quantum computing can enhance portfolio risk optimization and fraud detection at financial institutions, including through an improved Monte Carlo method of randomization. (KPMG, 2022)

Materials science: Quantum computing could provide insights that lead to the development of new manufactured materials, yielding higher energy storage in batteries for example. (Physical Review A, 2022)

Logistics and optimization: Early applications of quantum computers have included optimization of supply chains and logistics such as routing and deliveries. (Q-CTRL, 2024)

FOR EACH OF THE FOLLOWING INFRASTRUCTURE AND HARDWARE TECHNOLOGIES, WHAT BEST DESCRIBES YOUR SPENDING PLANS?



RESPONSE

Put yourself in a position to harness superposition

The promise of quantum computing is great, but when it will be delivered is uncertain. In the meantime, organizations can prepare to be first movers – or at least fast followers – when the technology makes a breakthrough and make an exponential leap in advantage.

BEYOND KEEPING UP WITH DEVELOPMENTS IN THE FIELD, IT LEADERS CAN TAKE SOME ACTIONS TO PREPARE:

Identify potential use cases: IT leaders educated about the capabilities of quantum computers can work with business leaders to identify where they could bring the most benefit. Identifying what types of problems the organization is most interested in leveraging quantum computing for will help guide investment decisions relating to vendors and business priorities. "There's a risk/reward trade-off you have to make in order to be leaders in the industry. Identifying the appetite for risks in order to reap the rewards is important and getting the business buy-in is crucial," says Gaylen Bennett, with IBM Quantum Industry & Technical Services.

Build quantum capabilities: CIOs will need the right talent from a limited pool to develop quantum algorithms and work with new quantum development frameworks. Relationships can be created with vendors to get access to resources early on and expand upon an organization's internal resources.

Manage stakeholder expectations: Investment in quantum computing in 2025 will take years to realize any return. IT leaders must be clear this is an experimental field and the organization is building its muscle now to be able to flex its might in the future. Work to educate stakeholders on where quantum computers will be useful and where they won't. "Quantum is not ready for production, so it's important to manage expectations while showing progress toward different milestones," says Imed Othmani, Industry Partner, Quantum Industry & Technical Services at IBM. (Interview with Bennett and Othmani)

> **"QUANTUM IS NOT READY FOR PRODUCTION, SO IT'S IMPORTANT TO MANAGE EXPECTATIONS WHILE SHOWING PROGRESS TOWARD DIFFERENT MILESTONES."**
>
> **IMED OTHMANI,**
> **INDUSTRY PARTNER, QUANTUM INDUSTRY & TECHNICAL SERVICES AT IBM**

THE INDUSTRIES BETTING ON QUANTUM

Our survey data shows that organizations in the media, information, telecom, and technology sector are most commonly investing in quantum computing by the end of 2025, with one in three indicating this. That is followed by public sector organizations at 27%, financial services at one in five, and education at 13%.

Top industries investing in quantum computing by the end of 2025

1. Media, Information, Telecom & Technology: 33% (n=61)
2. Government/Public Sector: 27% (n=111)
3. Financial Services: 20% (n=64)
4. Education: 13% (n=58)

*Not including industries where respondents were less than 10% of total group. Numbers are rounded to the nearest whole integer.

EXPLORE THE QUANTUM CLOUD OR QUANTUM COMPUTING AS A SERVICE

Most firms' first experience with quantum computing will come via access through cloud computing. Hyperscale cloud providers and specialized startups are offering this service model for customers today. Here's a few of the most notable services available today:

IBM Quantum: Developers can access 127-qubit quantum computers, including through a free tier, and use the Qisket framework or a GUI to interface with them.

Google Quantum AI: Offers superconducting qubit computers, similar to IBM's, and quantum computing simulators. The focus is on developing quantum-specific algorithms for the hardware used by researchers who widely share their findings with the community.

Amazon Braket: This fully managed service from Amazon Web Services provides access to different varieties of quantum hardware and simulators. Users pay as they go to run algorithms on the hardware for experimental purposes.

Microsoft Azure Quantum: Provides access to a variety of quantum computer solutions and hardware for the purposes of experimentation.

Alibaba Cloud: In partnership with the Chinese Academy of Sciences, Alibaba offers access to quantum simulators and a development platform for quantum algorithms. An emphasis is placed on open-source initiatives.

D-Wave: Specializes in quantum annealing technology that is best suited for optimization problems. Was early to market with its solution and has deployed to enterprise customers. Offers access to services through its Leap quantum cloud service and other large cloud providers.

Xanadu: Offers cloud access to programmable photonic quantum computers. Offers a full-stack Python library code-named Strawberry Fields for leveraging photonic quantum computers.

(The Quantum Insider, 2022).

TREND 03 | QUANTUM ADVANTAGE

EXAMPLES

The examples of organizations putting quantum computers to work today come from global brands with well-resourced research and development departments.

XPRIZE QUANTUM APPLICATIONS SPONSORED BY GOOGLE QUANTUM AI AND GENEVA SCIENCE AND DIPLOMACY ANTICIPATOR (GESDA) FOUNDATION.

The XPRIZE Foundation puts up cash prizes to incentivize research breakthroughs that solve humanity's biggest challenges and is offering a $5 million prize purse for researchers who can craft algorithms to help solve real-world challenges. Registration for the contest ended July 31, 2024, and by 2027, XPRIZE and the prize sponsors hope at least one winner will demonstrate quantum advantage for solving a real-world problem that benefits society. The contest was created for two main purposes, according to organizers: to accelerate the development of quantum algorithms that can solve practical problems and to accelerate solutions for big challenges that humanity is facing, like those encompassed by United Nations' Social Development Goals (UN SDGs).

Our analysis of quantum algorithms in development "found that applications were dominated by banks, aerospace, defense areas and lacked societal benefit potential. We aim to encourage a focus on global challenges such as public health, food security, and climate change mitigation to ensure the application opportunities of the technology are accessible to all. In Geneva, we are close to the UN SDGs and we had confirmation from UN organizations that there's a need to bring in disruptive science and tech to the scope of solutions that could be used to solve global challenges. Therefore, we wanted to create a prize with GESDA backing it." – Marieke Hood, Executive Director Impact Translator, GESDA

It was anticipated in mid-July that hundreds of teams would participate in the contest, with 440 teams from 63 different countries initiating the registration process. A mix of individuals, university-based teams, commercial startups, non-profit organizations, and other commercial enterprises compose the field. There's no guarantee the prize will be awarded – XPRIZE competitions have gone without a winner in the past. This one is particularly ambitious, as it seeks an algorithm that would prove quantum advantage perhaps even before quantum computing hardware is ready to support it. For example, while the contest concludes in 2027, IBM isn't projecting its commercially available quantum computers to achieve clear quantum advantage until 2029. But competitors will not have to run their algorithms on hardware to succeed – they will need to mathematically demonstrate the advantage of their algorithm on a stated quantum computing tool. A panel of judges will determine if the proof is valid.

"It's risky, but it's meaningful. That translates into commercialization in my opinion," says Kathrin Spendier, Technical Prize Director for XPRIZE Quantum Applications. "If you want to be a part of shaping quantum computing algorithm development in your particular area, you should start now."

Competitors may focus on solving problems related to public health, food security, or climate change mitigation. It is anticipated that most submissions will be geared toward algorithms designed for fault-tolerant quantum computers, which are expected to become available within the next five years or so. Submissions that propose algorithms for Noisy Intermediate-Scale Quantum (NISQ) devices are also welcome. Competitors aren't mandated to use any particular variety of hardware or quantum platform. But algorithms demonstrating versatility and adaptability to be run on different types of quantum architecture would be preferred. (Interview with Hood and Spendier)

> "THERE ARE CERTAIN PROBLEMS WE CAN'T SOLVE TODAY, BUT WE THINK WE CAN SOLVE IN THE FUTURE AND DO IT FASTER AND BETTER,"
>
> IMED OTHMANI,
> INDUSTRY PARTNER, IBM QUANTUM INDUSTRY & TECHNICAL SERVICES.

CLEVELAND CLINIC EXPLORES HEALTHCARE WITH ONSITE QUANTUM COMPUTER.

IBM plans to have eight of its 127-qubit System Two quantum computers deployed via a managed offering to client sites by the end of 2024. Cleveland Clinic will be one of those sites, deployed in December 2023. While most customers are experimenting through cloud access to quantum computing, some advanced clients can benefit from on-premises systems. This approach offers tighter integration with existing infrastructure and some advantages for data security considerations and provides hands-on experience with quantum computers to foster skills within the organization.

Ongoing research projects involving the system include:

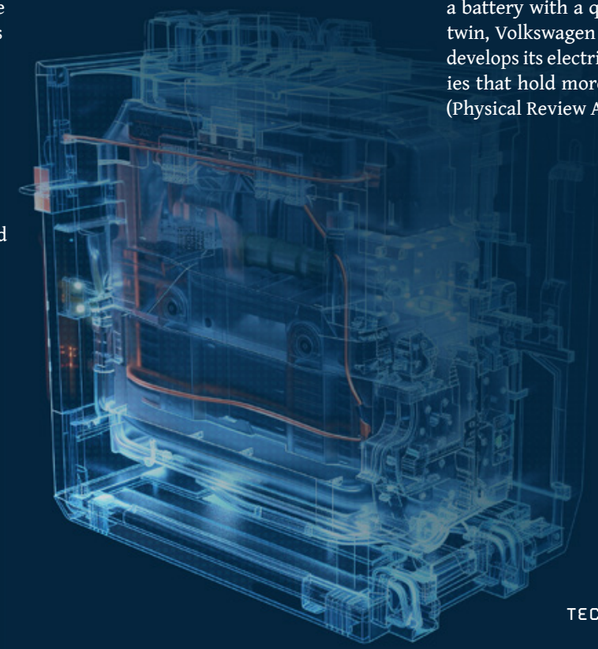
- Studying the risk factors for cardiovascular complications following non-cardiac surgery with quantum machine learning.
- Engineering optimal immune T-cells and immune T-cell receptors that are highly efficient at killing cancer cells using quantum computing and AI.
- Predicting protein structures more accurately and quickly, potentially leading to more insights on how proteins function and interact with other molecules. This in turn could lead to developing more effective and targeted therapies.
- Development of photon-activated drugs for cancer. Working with Algorithmiq's quantum-computing powered drug discovery platform, Aurora, the project will explore relevant drug applications.

(Cleveland Clinic)

BOEING SEEKS SOLUTION TO ECONOMY-SAPPING CORROSION.

Anyone that's ever owned a vehicle long enough is familiar with corrosion, the slow and inevitable damage done to metals over time as they are exposed to the environment. Whether it's rust or another variety of corrosion, it eats away at the structure and eventually makes it unusable. The problem is so widespread that it costs the worldwide economy an estimated 4% of GDP every year. Aerospace engineering firm Boeing wants to change that, and it's working with IBM to investigate quantum computing to better understand corrosion mechanisms. Eventually, simulations could lead to new materials that are more resistant to corrosion or new treatments and design strategies to prevent corrosion. (Interview with Bennett and Othmani)

"There are certain problems we can't solve today, but we think we can solve in the future and do it faster and better," says Imed Othmani, Industry Partner, IBM Quantum Industry & Technical Services.



HSBC EXPLORES QUANTUM APPLICATIONS IN FINANCIAL SERVICES.

The London-based bank works with several quantum computing solution providers and its own dedicated quantum research team of in-house PhDs to formalize use cases in the financial services industry. HSBC seeks to develop patents in the space and collaborates with its lines of business to identify practical use cases while improving processes in preparation of a quantum-powered economy. High-potential use cases include price optimization for trading, with a proof of concept (PoC) in the works to provide real-time and flexible pricing options. Another PoC will look at optimizing collateral allocation. (HSBC)

VOLKSWAGEN SIMULATES ELECTRIC CAR BATTERY.

Working with Toronto-based quantum computer provider Xanadu, the German automaker estimated the resources required to simulate a lithium-ion battery with a quantum algorithm. By simulating a battery with a quantum-powered digital twin, Volkswagen could change the way it develops its electric cars and provide batteries that hold more charge and last longer. (Physical Review A, 2022)

04

TREND/04

POST-QUANTUM CRYPTOGRAPHY

→ Migrate to quantum-resistant encryption before it's too late_

/ imagine
a top-down shot of an abstract image based on the concept of cryptography lattices and quantum computing using millions of voxels, dramatic lighting, blues and pinks, 3D render --style raw --v 6.0 --ar 17:11

TREND 04 | POST-QUANTUM CRYPTOGRAPHY

THREAT

Countdown to Q-day

The IT industry is counting down to Q-day – an uncertain day in the future that will mark the point when quantum computers can break public-key encryption within 24 hours. We don't know when it will arrive, but we do know it will happen eventually. Will we plan to mitigate the risks of it accordingly? Rather than being a "black swan" crisis that takes the industry by surprise, Q-day could be a "grey rhino" event that we see coming from a distance yet fail to prepare for properly.

Public-key encryption standards such as RSA are widely used across all industries and are the standards that allow for the safe transmission of data over the internet or in storage and for secure authentication with permissioned users. They depend on mathematical algorithms, such as prime factorization, that classical computers are very inefficient at solving to provide security. But quantum computers executing prime factorization will eventually make cracking that code trivial, rendering this type of encryption obsolete. Operating with RSA encryption after Q-day will be equivalent to storing all data without any encryption today – an unacceptable situation for privacy and security. Industries that are accountable to protect sensitive data will be the most affected by this reality, including finance, healthcare, telecommunications, and government.

How long do we have? It's a matter that's up for debate. In a survey of quantum computing experts conducted by the Global Risk Institute, more than a quarter of quantum computing experts rate a likelihood of 50% or more that Q-day will arrive in the next ten years. More than half of experts say it's 50% likely or more within the next 15 years. This represents a level of risk that many organizations consider actionable. "Estimates may correspond already to an interoperable risk that needs to be mitigated through immediate action," states Global Risk Institute (2023). One such organization requiring immediate action is the Department of Homeland Security. In its view, the likelihood of a quantum computer breaking encryption standards is likely enough by 2030 that all government agencies should be making plans to migrate to quantum-resistant cryptography right now (Department of Homeland Security, 2021). In fact, the Quantum Computing Cybersecurity Preparedness Act requires organizations to complete their plan for migration within one year of the NIST release of its post-quantum cryptography standards (117th Congress, 2022).

Prior to the NIST standards being released, planning a migration to post-quantum cryptography was difficult because the techniques to accomplish it were unclear. But with the release of the first three post-quantum cryptography standards on August 13, 2024, NIST completed its multi-year process to replace its most vulnerable current encryption standards, including digital signatures. Even with more standards to be released in the future, this provides the IT industry with guidance required to put the upgraded encryption into practice.

There is reason to act with greater urgency in migrating encryption standards beyond the possibility of a quantum-computer attack in five to ten years. A "Harvest Now, Decrypt Later" attack involves bad actors stealing important encrypted data now with plans to decrypt it in the future when quantum computing makes it possible. So even today, sensitive data is vulnerable to a well-planned quantum-computing attack in the future. (Global Risk Institute, 2023)

"ESTIMATES MAY CORRESPOND ALREADY TO AN INTEROPERABLE RISK THAT NEEDS TO BE MITIGATED THROUGH IMMEDIATE ACTION."

GLOBAL RISK INSTITUTE, 2023

/ imagine
a storm slowly making its way over a modern business district, the overall atmosphere should be foreboding --style raw --v 6.0 --ar 3:4

TREND 04 | POST-QUANTUM CRYPTOGRAPHY

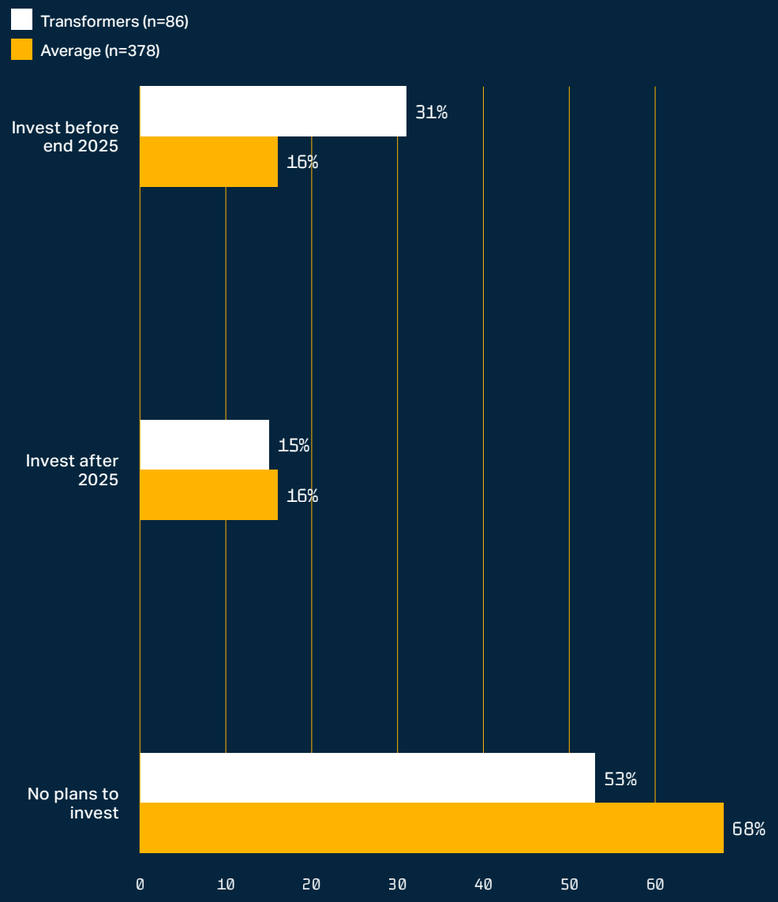
MITIGATION

Make like a butterfly and migrate

Mature IT organizations are investing in post-quantum cryptography before the end of 2025 at nearly twice the rate of average IT departments. Transformers reported plans to invest before the end of 2025 31% of the time, while average departments only did so 16% of the time. Plans to invest in 2025 were about equal, with 15% of Transformers reporting so and 16% of average departments. Many organizations have no plans to invest in post-quantum cryptography yet, with 53% of Transformers reporting this is the case and two-thirds of average departments.

An industry breakdown of investment in post-quantum cryptography reveals that the public sector is not yet prioritizing it as highly as other critical infrastructure industries. Given that NIST's standards are now available and the one-year countdown to submit an encryption migration plan is started, it's surprising to see they are behind other industries.

DOES YOUR INVESTMENT IN CYBERSECURITY INCLUDE ANY INVESTMENT IN POST-QUANTUM CRYPTOGRAPHY?



GET TO KNOW YOUR POST-QUANTUM ENCRYPTION STANDARDS

NIST finalized three post-quantum cryptographic algorithms on August 13, 2024. Two of them were developed by IBM researchers in collaboration with several industry and academicpartners, the third algorithm was co-developed by a researcher that has since joined IBM (IBM Newsroom, 2024). The finalized encryption standards are meant to replace widely used public-key encryption systems. NIST didn't make any substantive changes to the standards since the draft versions but did change the names of the algorithms.

Standard	New Algorithm Name	Old Algorithm Name	Advantages	Application
FIPS 203 (Federal Information Processing Standard)	ML-KEM, short for Module-Lattice-Based Key-Encapsulation Mechanism	CRYSTALS-Kyber	Comparatively small encryption keys that two parties can exchange easily as well as its speed of operation.	General Encryption
FIPS 204	ML-DSA, short for Module-Lattice-Based Digital Signature Algorithm	CRYSTALS-Dilithium	Offers three options for security strength based on needs. Can be used for a variety of applications including email, funds transfer, and software distribution.	Protecting Digital Signatures
FIPS 205	SLH-DSA, short for Stateless Hash-Based Digital Signature Algorithm	SPHINCS+	Intended as a backup method in case ML-DSA proves vulnerable.	Protecting Digital Signatures
FIPS 206* (Not yet finalized, expected late 2024)	FN-DSA, short for FFT (fast Fourier transform) over NTRU-Lattice-Based Digital Signature Algorithm	FALCON (Fast Fourier lattice-based compact signatures over NTRU)	The most compact of all post-quantum signature schemes and "quite fast."	Protecting Digital Signatures

TREND 04 | POST-QUANTUM CRYPTOGRAPHY

MITIGATION (CONT'D)

Info-Tech offers a gameplan for planning your migration with a five-phase approach in *Prepare for Post-Quantum Cryptography*. In short, organizations are recommended to:

1. **Prepare.** Get buy-in from the leadership team and educate your team about the threat faced and the transition.
2. **Discover.** Take stock of your vulnerable systems, data, and applications. Create an inventory of all these use cases.
3. **Assess.** Consider the security risks posed by quantum computing on your own organization and assess your readiness to transform existing encryption methods.
4. **Prioritize.** Consider what data and systems are most sensitive, which will require the greatest lead time to prepare, and create a roadmap for encryption transformation.
5. **Mitigate.** Implement the post-quantum cryptography standards and decommission old technology and systems that are obsolete. Test products that use the new standards.

If you're wondering how your state of readiness for post-quantum cryptography compares to your peers, we've organized our respondents into tiers based on their investment plans. It's interesting to note that while the US federal government will be required to make a plan in the near term, government and the public sector as a whole is behind other industries in investing.

Tier 1 reflects industries that perhaps have the most to lose when current encryption methods become obsolete. Financial services wouldn't be able to protect tampering with trading platforms for example. Telecom and technology firms could also see their customers' data intercepted in mid-stream and decoded. Such scenarios threaten not only the companies offering these types of services but also the global economy as a whole.

THREE TIERS OF READINESS FOR Q-DAY

*indicates low response sample for this question from marked industries. All numbers rounded to nearest whole, rows may not equal 100%. *n*=545

TIER 1: WE'D BETTER FIX THIS NOW

Industry	Investing before end of 2025	Investing after 2025	No plans to invest
Financial Services	28%	16%	57%
Gaming & Hospitality*	40%	10%	50%
Media, Information, Telecom & Technology	20%	23%	37%
Natural Resources*	37%	25%	38%

TIER 2: WE'LL GET TO IT NEXT YEAR

Industry	Investing before end of 2025	Investing after 2025	No plans to invest
Healthcare & Life Sciences	13%	20%	67%
Manufacturing	20%	13%	67%
Utilities*	18%	24%	59%

TIER 3: MAYBE WE HAVE UNTIL 2035

Industry	Investing before end of 2025	Investing after 2025	No plans to invest
Government/ Public Sector	11%	30%	65%
Professional Services	13%	7%	80%
Retail & Wholesale*	11%	11%	78%
Education	20%	14%	66%

TIER 4: MAYBE WE HAVE UNTIL 2035

Industry	Investing before end of 2025	Investing after 2025	No plans to invest
Real Estate and PropertyManagement*	0%	25%	75%
Construction*	11%	0%	89%
Arts & Entertainment*	0%	0%	100%

TREND 04 | QUANTUM UTILITY

EXAMPLES

Quick to quantum-resilient security

Despite the most widely used types of current-day encryption not yet having quantum-resistant replacements standardized and ready to deploy, many companies in the technology and telecom sectors have an early start on the migration. In other cases, technologically sophisticated enterprises are working with technology partners to test quantum-resistant security methods and begin learning about how to operate in this new paradigm.

In some contexts, first movers in this space are using already standardized post-quantum cryptography standards from NIST that are appropriate for more niche use cases. In others, they are working with the draft standards NIST has made available.

HP RELEASES FIRST QUANTUM-RESISTANT LAPTOPS.

HP Inc. announced that it is the first PC-maker to protect on-board firmware with post-quantum cryptography, releasing the commercial laptops to general availability in March and April. HP embeds its encryption directly on silicon with its Endpoint Security Controller (Gen 5) chip. It prevents corrupted or malicious updates for systems' firmware or BIOS. Certain notebooks from the ProBook and EliteBook series include the chip. HP developed the encryption by using an already available NIST standard: Leighton-Micali Signature Scheme (LMS). LMS wouldn't suit many uses cases because it uses longer encryption keys that are slower to unlock and there are a finite number of keys that can work in the system's lifetime – once they've been exhausted, the system can no longer be used. Thus, systems that require thousands to millions of exchanges can't rely on this standard, but HP knows it will only update its laptop firmware dozens of times over a system's lifespan. HP also gets the advantage of using a robust method that is already standardized, rather than taking the risk of using a draft standard that would be permanently inscribed into its silicon. (Interview with Ian Pratt)

"If you can compromise a PC at the firmware level, all bets are off from a security point of view. You've got an attack that would be easy to deploy but would be very difficult to detect and would give you effectively full control over that system." – Ian Pratt, Global Head of Security for Personal Systems at HP Inc.

SK TELECOM TESTS QUANTUM-RESISTANT MOBILE NETWORK.

The Korean mobile operator is working with digital security vendor Thales to deploy PQC on its 5G networks and SIM cards. The collaboration would see subscriber data encrypted and decrypted in a quantum-resistant approach on the telecom provider's 5G standalone network. (Thales Group, 2023)

HSBC TESTS QUANTUM-SAFE FOREX.

In partnership with Toshiba, HSBC is the first bank to join the London commercial quantum secure network, which will test deployment of quantum key distribution, a method of encryption that leverages quantum computing to keep data secure. HSBC conducted a test of the system to complete foreign exchange currency trades. (Toshiba, 2024)

CLOUDFLARE OFFERS FREE QUANTUM-RESISTANT WEB SERVICES.

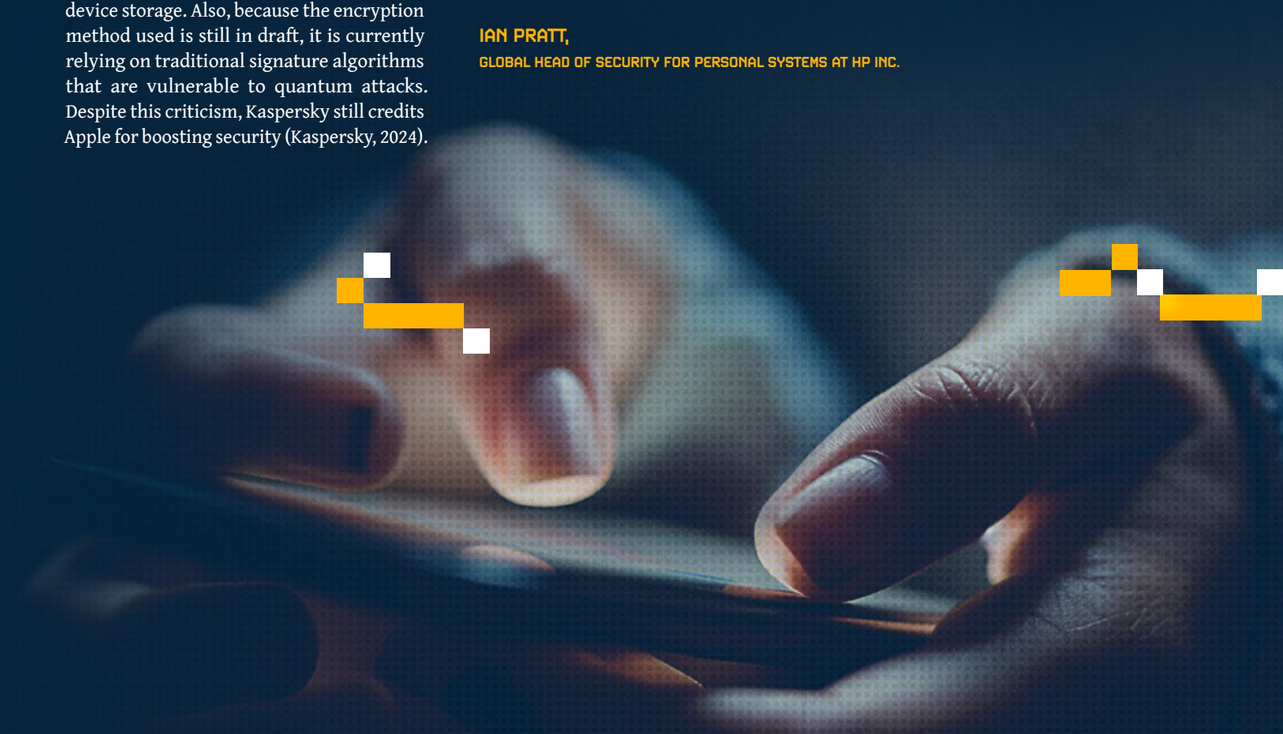
Cloudflare offers customers internet infrastructure services such as a content delivery network and a domain name system resolver. Starting in October 2022, it enabled a beta offering, delivering post-quantum cryptography encryption for all websites and APIs that it services. This requires a web browser that supports post-quantum cryptography, and Google Chrome began enabling this standard by default in August 2023. Cloudflare says it has upgraded many of its internal connections to be quantum-resistant and plans to complete its work by the end of 2024. After that, the focus shifts to encrypting traffic on outbound connections. Cloudflare was able to begin its process early by working with NIST's draft standard for post-quantum cryptography, and when the final standards are released, Cloudflare will shift to support them. (Cloudflare, 2023)

APPLE BRINGS QUANTUM-SECURITY TO IMESSAGE.

Apple announced an iMessage upgrade on February 21, 2024, which included post-quantum cryptography protection based on a NIST draft standard. Apple acknowledged that it wanted to protect against "Harvest Now, Decrypt Later" attacks that see attackers steal encrypted data and file it away for future use (Apple Security Research, 2024). However, a Kaspersky blog post criticized the measure as inadequate to protect against quantum computer attacks because it only protects the transport layer of messaging. The message could still be retrieved from device storage. Also, because the encryption method used is still in draft, it is currently relying on traditional signature algorithms that are vulnerable to quantum attacks. Despite this criticism, Kaspersky still credits Apple for boosting security (Kaspersky, 2024).

"IF YOU CAN COMPROMISE A PC AT THE FIRMWARE LEVEL, ALL BETS ARE OFF FROM A SECURITY POINT OF VIEW. YOU'VE GOT AN ATTACK THAT WOULD BE EASY TO DEPLOY BUT WOULD BE VERY DIFFICULT TO DETECT AND WOULD GIVE YOU EFFECTIVELY FULL CONTROL OVER THAT SYSTEM."

IAN PRATT,
GLOBAL HEAD OF SECURITY FOR PERSONAL SYSTEMS AT HP INC.



/ imagine
a pharmaceutical capsule full of tiny glowing nanites, floating on a dark background, --style raw --v 6.0 --ar 2:1

WHAT'S NEXT?

1

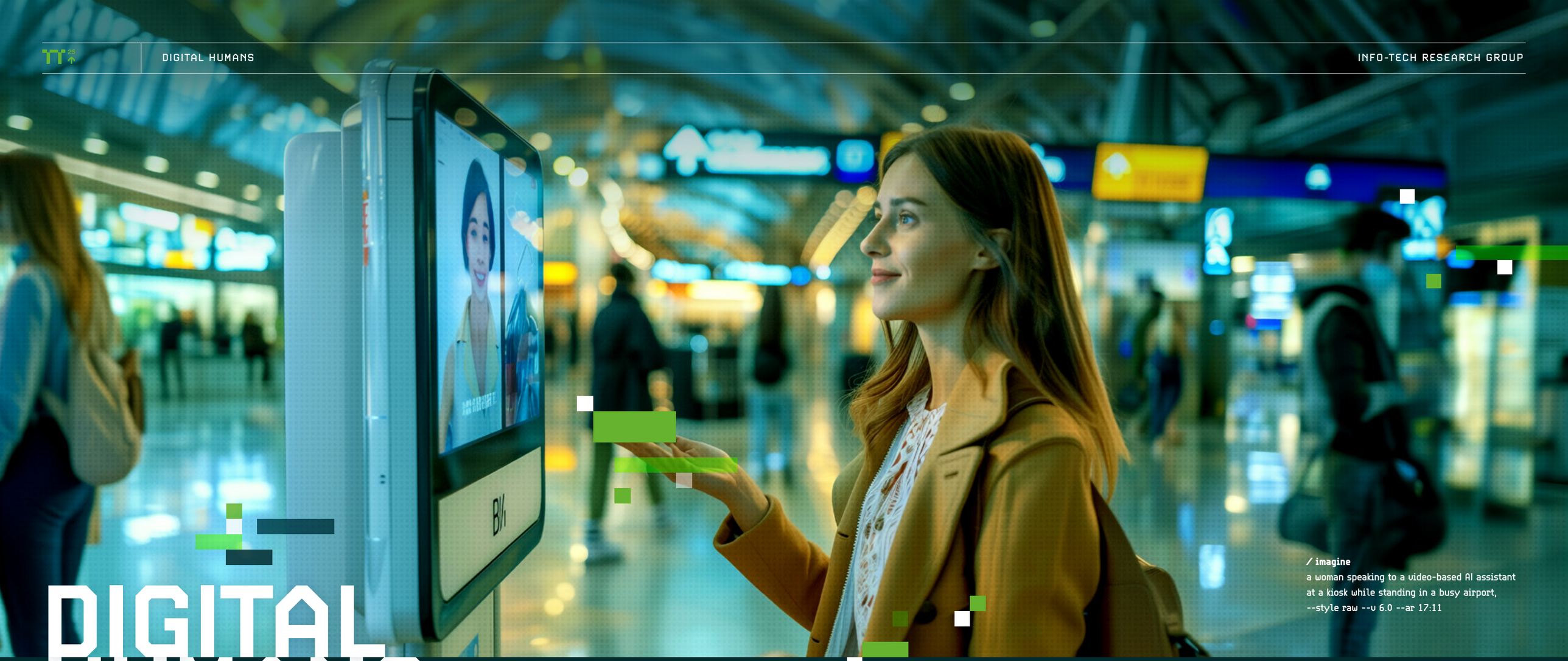
Experimentation of quantum computing using real-world business problems will be the focus during the era of quantum utility, with organizations in industries with the most to gain from finding a quantum advantage leading the way – including finance, technology, and healthcare/pharmaceutical.

2

By 2026, at least one-third of all organizations will be investing in post-quantum cryptography. By 2030, at least one-half of all organizations will be investing in post-quantum cryptography.

3

When quantum advantage is achieved and available through cloud computing, it will spur a massive increase in investment across many more industries.



/ imagine
a woman speaking to a video-based AI assistant at a kiosk while standing in a busy airport, --style raw --v 6.0 --ar 17:11

DIGITAL HUMANS

Generative AI pushes beyond the Turing Test

People can no longer tell the difference between a chatbot and a human being. The Turing Test has long been the standard by which computers are evaluated in terms of approximating human intelligence. In a recent study at UC San Diego, participants were asked to have a five-minute text-based conversation with another party and then guess if it was a human or a machine. Participants correctly identified humans 67% of the time, but OpenAI's ChatGPT models also did quite well. ChatGPT 3.5 was identified as human half the time, and GPT-4 was identified as human 54% of the time. In other words, being able to identify a human from a machine was no better than chance. (Inc., 2024)

Not only does the ability of a large language model (LLM) to pass the Turing Test mean that we'll need to design new CAPTCHAs to separate man from machine on the internet, but it begs the question, should people know when they're interacting with a person or a machine while going about their business? Or if an LLM can imitate a person so convincingly in many different contexts, can we now use AI to do some things that people used to do?

It's not just text-based interactions that are up for grabs by digital simulacra. Voice cloning technology is bringing distinct human voices that can be rendered into recorded works or generated in real-time. Video and 3D graphics rendering is also advanced enough that realistic visual digital twins are nearly indistinguishable from the real people. Generative AI is capable of creating digital twins in many different modalities, and as a result, the global market is booming exponentially, expected to grow from US$10 billion in 2020 to a value of US$530 billion in 2030 (Synthesia, 2024).

While commercial opportunities created by digital humans will positively impact many industries, the adverse impact of easily generated deepfakes poses a grave threat to society that is now more acute than ever.

AI industry observers have long warned about the inevitable threat of convincing "deepfakes" that can't easily be distinguished from real people. They have arrived and are already being exploited globally by cybercriminals for fraud and in cyber-misinformation campaigns to create political influence, especially related to elections.

As companies contemplate how and when digital humans will play a role in their operations, they'll also need to adopt new mitigations to contend with the new cyberthreats created by the very same technology.

TREND/05

AI AVATARS

→ Simulate human interaction across channels _

/ imagine
a DNA strand dissolving into brightly colored particles, 3D render --style raw --v 6.0
--ar 17:11 --v 6.0

TREND 05 | AI AVATARS

OPPORTUNITY

You're awfully chatty: Chatbots are proliferating

In last year's Tech Trends report, we examined how many enterprise software vendors were revamping their user interfaces with generative AI-powered chatbots. From Microsoft Copilot to Salesforce Einstein to Amazon Q to myriad more options, both proprietary and open source, it seems as though a natural language interface is becoming the default mode of interaction between users and software. You might say it's less point and click, more chat and go.

Consider that even Google is overhauling its own search engine with its Gemini AI, and Microsoft includes Copilot chat on its Bing home page. Search is the most common technology interaction that human beings have, with an average of 8.5 billion Google searches a day (SEO.ai, 2024). Now that interaction will be mediated by an LLM.

Generative AI chatbots facilitate good user experience by interacting with users like they would interact with their co-workers – conversationally. They cut through arcane icon and menu interfaces that sometimes represent hundreds of different features, providing a user exactly what they ask for. They are particularly good and finding relevant knowledge and summarizing it and can sometimes even generate exactly what the user needs to complete a task.

Yet there are downsides. They are prone to errors and can be biased by training data. As we'll cover later in this theme, they open up users to risks around data confidentiality, performance problems, or inflating costs. This may explain why we saw some hesitancy among respondents in last year's Tech Trends report to adopt generative AI features as soon as they were made available, with most preferring to let others test them out first.

SONIC SIMULACRA: AI FINDS ITS VOICE

Generative AI makes high-quality voice cloning easy to achieve. With a few minutes of training from a voice actor, new audio can be generated from a text script and sound very similar to the real actor. Controls can add variance to the speed, pitch, and tone of the generated voice. Not only is the quality better, but the speed of generation is improved to the point that it can be generated in real-time. Traditionally, generated AI voice has been mostly used in prerecorded materials, but now it can be leveraged in more dynamic and interactive environments.

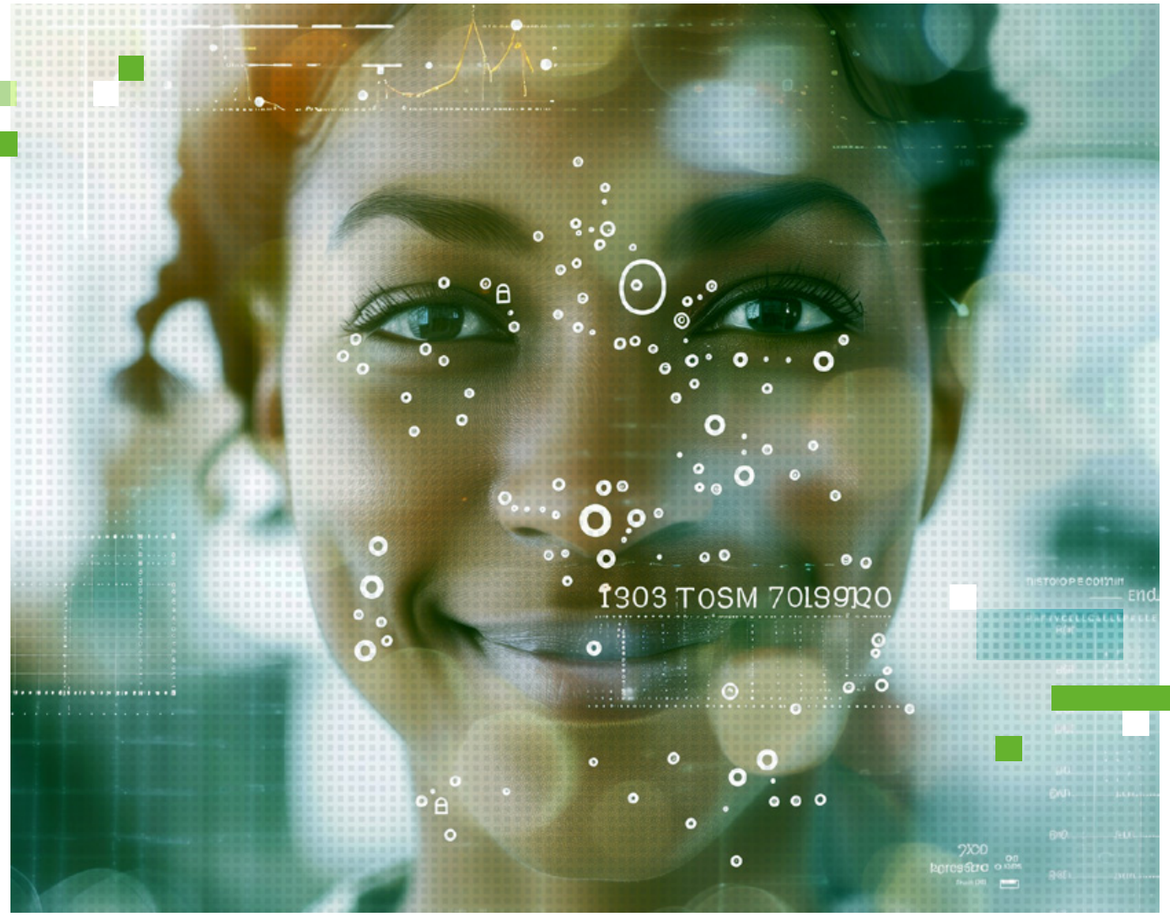
The global AI voice generator market is estimated to grow at a rate of 15.4% per year from 2022 to 2032, with a projected value of almost US$1.9 billion in 2025 and US$4.9 billion by 2032. Most voice content will be generated in the cloud during that period, opposed to on-premises solutions. More than half of the demand will be created by the advertising and media industry, but healthcare will be the industry with the second-most demand, generating about one-fifth of it. Other industries leveraging AI voice include manufacturing, retail, automotive and transportation, and financial services. (Market.us, 2023)

Voices.com bills itself as the #1 voice-over marketplace on the internet. It's pursuing an AI-driven strategy in partnership with its voice talent (more than four million creators) because Voices.com CEO Jay O'Connor sees a massive opportunity to inject new revenue into a mature market.

> "WE BELIEVE AI SIMULTANEOUSLY POSES A THREAT AND A MASSIVE OPPORTUNITY FOR VOICE ACTORS AND THE VOICE COMMUNITY AS A WHOLE."
>
> JAY O'CONNOR
> CEO, VOICES.COM

"It introduces a broad set of new use cases that is going to entirely transform the whole voice market," he says. "We believe AI simultaneously poses a threat and a massive opportunity for voice actors and the voice community as a whole."

Generative AI can produce new video frames or realistic digitally rendered 3D graphics that look just like real people. While the motion effect of this sort of generated content isn't perfect yet, it's at the point where a short video could fool a reasonable observer.



Synthesia and **Heygen** are two examples of vendors that offer cloud-based platforms where users can generate realistic video content with digital humans. On both platforms, users can either choose from a selection of digital humans and voices to create their videos or they can train their own AI avatar by uploading just a couple minutes of video. Different features are available to create prerecorded videos based on a script, with translations offered in a wide variety of languages, or to produce an interactive AI avatar that responds to prompts. Users need to authenticate their own identity and that of other individuals they will create AI avatars for on these platforms. Info-Tech leveraged this technology to create an AI avatar of its keynote speaker Rob Meikle for its Las Vegas-based LIVE event in September.

Synthesia's CEO Victor Piarbelli says his company produces 3,000 videos daily. Organizations use the videos for different purposes ranging from internal training and customer service to sales prospecting (Harvard Business Review, March 2023).

Epic's Metahuman creator is a digital tool that can render realistic-looking humans for the software vendor's Unreal Engine, used by many video game creators and, in some cases, for enterprise use cases. The tool allows for precisely rendered 3D graphics to be matched with motion capture data – including facial expressions – that can be recorded with consumer-grade hardware – even an iPhone. (Epic Games, 2024)

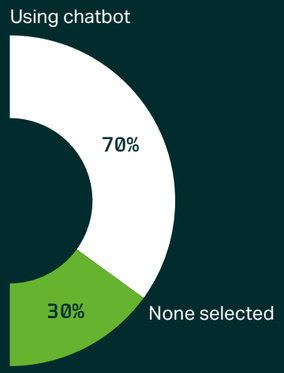
TREND 05 | AI AVATARS

RESPONSE

Meet your new AI colleagues

It's a year after organizations mostly told us they'd rather see others test out new generative AI features released by vendors. With many chatbots on the market, how are IT leaders responding now? It seems that for the most part, organizations have moved past their hesitancy.

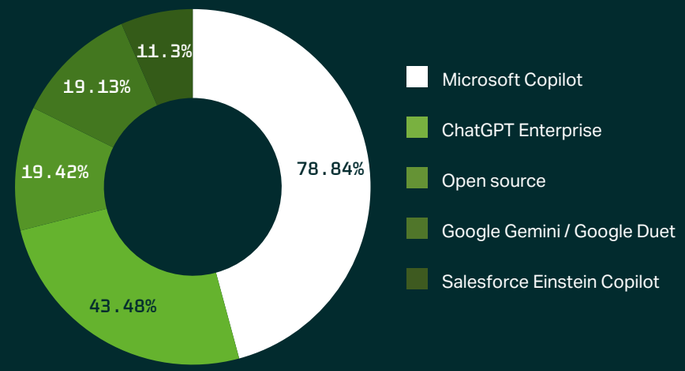
DOES YOUR ORGANIZATION CURRENTLY USE OR PLAN TO USE ANY OF THE FOLLOWING GENERATIVE AI CHATBOTS?



Most organizations are using at least one chatbot or are planning to deploy one, selecting one or more from a list we provided in the survey or selecting "other." Many of the options are easy to adopt, offered as upgrades to existing software packages or as simple subscription services for a web service. For example, Microsoft Copilot is a chatbot integrated with the software firm's Office 365 productivity suite. It dominates the field, with nearly eight in ten chatbot users saying they use it or plan to use it.

DOES YOUR ORGANIZATION CURRENTLY USE OR PLAN TO USE ANY OF THE FOLLOWING GENERATIVE AI CHATBOTS?

n=465, top 5 most popular selections shown



Microsoft licenses OpenAI's GPT models to support its chatbot but also has other license deals and its own developed models to field prompts. Another OpenAI-powered chatbot is the second most popular option, with ChatGPT Enterprise being selected by 44% of respondents. Open-source options – which may include models from Meta or Mistral – edge out Google Gemini for third place, with about one in five respondents selecting it.

Many respondents say they are using or planning to use multiple chatbots, with 73% selecting multiple options from our list of available chatbots.

Copilot and other new chatbots are used by enterprises to improve productivity in several different ways:

Software development: Copilot can provide either new code or auto-complete a string of code a human is writing. It can help debug code and overall help developers get more routine tasks completed more quickly.

Creating personalized content: From healthcare providers to marketing professionals, it's often the case that professionals want to tailor their message for the audience. With generative AI understanding both the user and the content available from an organization, a message can be tailored at the individual level in an automated fashion. Although, it's still wise to have a human in the loop to review content for quality and accuracy.

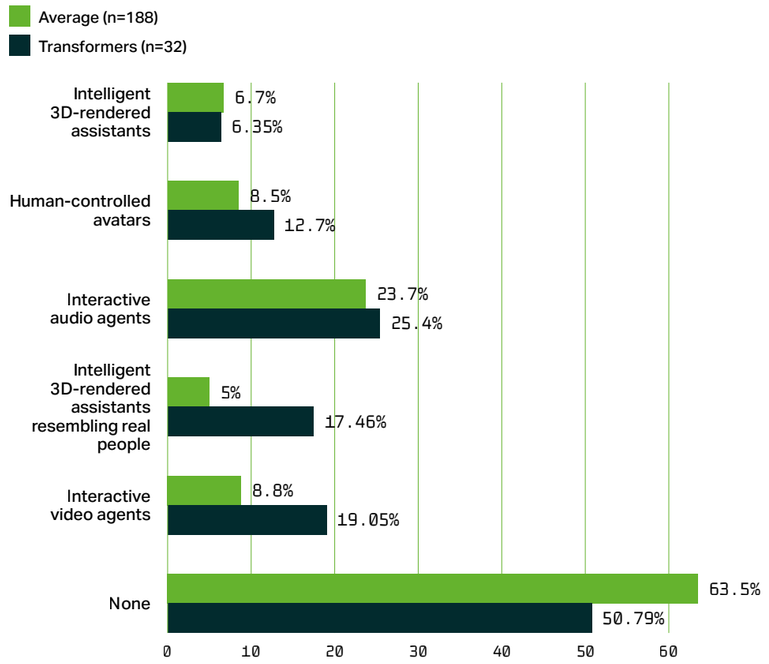
Legal communications: Poring over long documents written in legalese is tedious for any professional. Chatbots can help explain documents in plain language and highlight the most significant parts. Legal departments are finding that using generative AI to augment their work with legal documents can cut the time it takes in half.

Data analysis interpretation: While generative AI isn't the best at doing the math behind data analysis, it can be helpful in explaining results in plain language and turning natural language questions into the right data queries. It is often used to even create visual graphs of data. (US Cloud, 2024)

WHY TEXT WHEN YOU CAN TALK?

Many organizations are exploring the use of generative AI-powered agents beyond chatbots. More sophisticated IT departments are generally more interested in pursuing these agents in 2025 compared to an average IT department. Half of all Transformers say they are interested in an audio or visual AI agent in 2025, compared to just 36.5% of average IT departments.

BEYOND CHAT, WHAT TYPES OF VIRTUAL AGENT OR DIGITAL HUMAN IS YOUR ORGANIZATION MOST INTERESTED IN ADOPTING IN 2025?



Adding voice or video elements to an AI agent brings more of an emotional canvas to the interaction experience, and these technologies are being explored for different use cases than text-based chatbots:

Kiosk hosts: AI avatars are being deployed to onsite information kiosks at airports and malls to provide personalized directions and other information.

Companions: Several companies are providing paying customers with the ability to build an AI avatar and form a relationship with it. Users often report reduced anxiety and loneliness due to their interaction with a digital friend who is always accessible and never has plans other than to talk with their human. People have even entered open romantic relationships with their AI avatars and have staged weddings in virtual settings.

Entertainment: Some may form real relationships, but others will talk to AI agents more for entertainment. Voice agents can read audio books or other interactive stories. Visual avatars can play games or talk about an interesting topic. Digital humans will play a role in entertainment through social media, podcasts, audio books, film, television, and video games.

TREND 05 | AI AVATARS

EXAMPLES

Human reflections:
Building AI clones in voice and visual

The idea of digital simulacra pervading our economy and interacting with real humans would have been wild to most people even just a few years ago. Yet in 2025 it will become so commonplace that most people will start to expect that they'll encounter AI avatars as they go about their daily lives. Sometimes these digital humans will be twins, or clones, of real people. Other times, they will be totally fictional creations.

VOICES.COM SEES EXPONENTIAL OPPORTUNITY WITH AI VOICE

Founded in 2003 in London, Ontario, Canada, this software company has built an online marketplace of voice talent, with four million actors ready to hire for producers of commercials, TV shows, films, training videos, rich media websites, educational and training material, and other purposes. For 20 years, that hiring relationship was always between a producer and a human voice actor. But that changed in 2024 with the launch of Voices AI Studio.

Now voice actors can create clones of their voices to be licensed by clients. Voices started developing its platform with third-party AI models but soon recognized it could deliver benefits not available on the market by training its own. Clients just type their scripts, and the voice clone of their choice produces the audio. Clients are able to control the speed, tone, and inflection of the voice to match it with the desired emotion.

Voices says it is the largest source anywhere of voice clones from professional voice actors and that leading companies are sourcing and licensing their AI voices through the company. Top voice actors are being invited by Voices.com to create voice clones available for license right now. In the long term, CEO Jay O'Connor believes that the top half of talent on the platform could benefit from offering a voice clone. Just as with their rates for doing work, voice actors can set their rates and terms for licensing their voice.

The CEO is clear that Voices.com didn't leverage its talents' voice recordings without permission to train its AI model. Rather, actors were directly compensated for their work. Voices.com also sells its clients ethically sourced audio and video material so they can train their own AI models.

O'Connor declined to specify how client payments are divided between the talent and the platform but said "we are very generous."

In the future, Voices.com plans to offer a real-time conversational AI API product for clients interested in generating voice clone audio in real time.

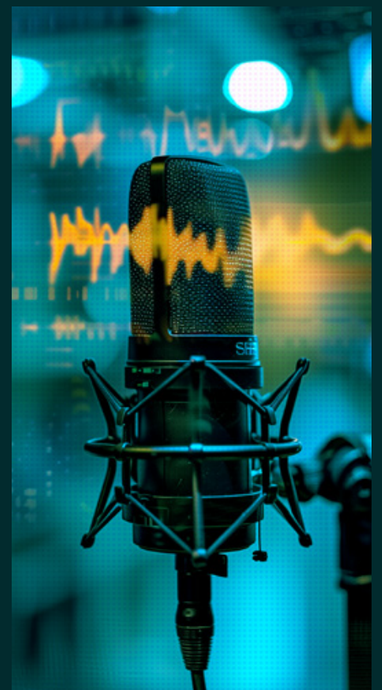
The CEO is excited for what AI could mean for Voices.com talent and its business.

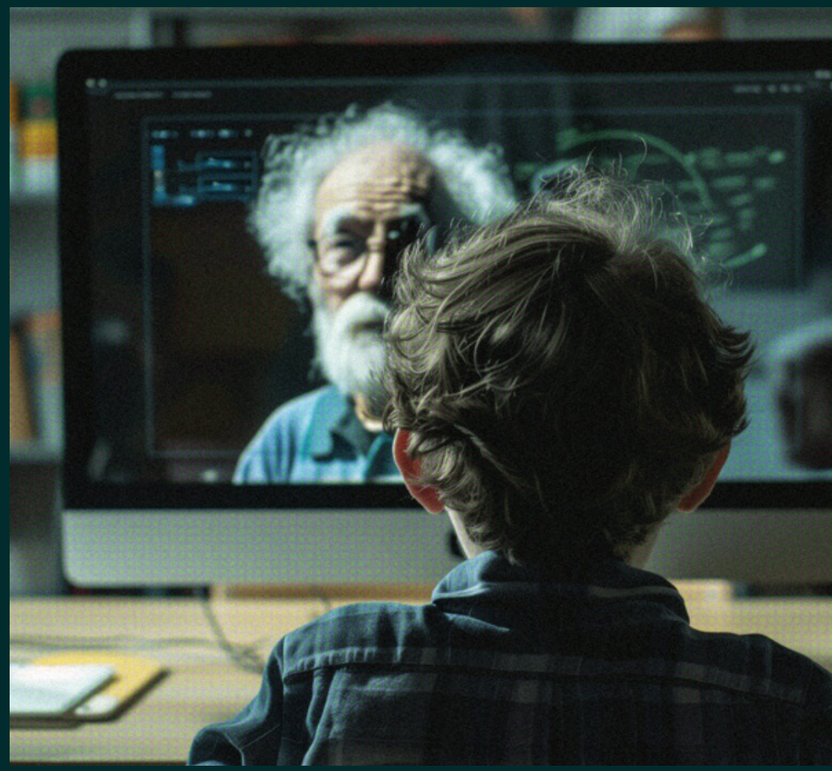
"Our growth is explosive right now," says O'Connor. He sees AI voice driving new clients to the platform and envisions a future where brands view a recognizable voice as indispensable. "Everyone wants their brand to be distinctive. So you want to license a voice that will represent your brand."

Also on the future roadmap is taking AI Studio beyond English into other languages.

"EVERYONE WANTS THEIR BRAND TO BE DISTINCTIVE. SO YOU WANT TO LICENSE A VOICE THAT WILL REPRESENT YOUR BRAND."

JAY O'CONNOR
CEO, VOICES.COM





WILLIAM SHATNER BOLDLY GOES INTO CONVERSATIONAL VIDEO AI

Star Trek's own Captain Kirk was cloned at least a couple of times throughout the '60s sci-fi series. And now the actor that portrayed him is getting the same treatment as William Shatner collaborated with **StoryFile**, an interactive platform, to put his own story on the front page of its website. The concept of StoryFile is that you can record videos with loved ones and use them to make interactive conversational AI to preserve their memory. Now 90, Shatner fields just about any question you can throw at him in this interactive video. He talks at length about his acting career, his family, and even his views on death. (Screenrant, 2021)

LIL MIQUELA IS AN AI INFLUENCER

Created by software firm **Brud**, Lil Miquela is a virtual influencer that's now 21 years old and has millions of followers on Instagram. Created in 2016, Lil Miquela has previously been named as one of the 25 most influential people on the internet (2018) and was estimated to be worth $10 million in 2023. Lil Miquela still posts her updates to Instagram regularly and often endorses products like fashion and food. (Cut The SaaS, 2023)

ARAB BANKING CORP. HIRES AI AS A PUBLIC FACE

Fatema is the AI avatar serving as the public face of the Bahrain-based bank. She regularly interacts with customers and appears on the bank's social media posts. Fatema debuted in 2019 and leverages Soul Machines' Digital DNA platform. "Fatema's synthetic makeup was produced from a digital gene pool, which allowed Bank ABC to choose specific traits and attributes to develop the optimal digital human for their organization," states a press release. (Bank ABC)

EINSTEIN AI BUT NOT SALESFORCE

Digital human platform **Uneeq** partnered with Hebrew University of Jerusalem and Greenlight Rights to create a digital version of Albert Einstein. The avatar answers questions about his life and work, providing an educational context about this important historical figure. (Uneeq)

06

TREND/06

DEEPFAKE DEFENSE

→ Counter AI-powered attacks_

/ imagine
extreme closeup of a cracked and damaged mask made of metal with gowing LED lights, with pieces missing, lying in the gutter of a street on a cold rainy night, 3D render --style raw --v 6.0 --ar 49:24

TREND 06 | DEEPFAKE DEFENSE

THREAT

"Seeing is believing" no longer applies

The AI tools used to create digital humans for legitimate business purposes, like those discussed above, have safeguards in place that require the consent of any individual that will be imitated by a clone. But other similar technology is available on the market, either via open-source licenses or perhaps sometimes hacked versions of proprietary software, giving bad actors access to this powerful capability as well. The result is that we are entering into an era where deepfakes – realistic digital imitations of real people – are going to exacerbate the misinformation problem on the internet and supercharge the phishing and social engineering tactics employed to commit fraud.

"Seeing is no longer believing. And that's really, really scary because you know for human beings, because of the way that our visual cognitive system works, we're hard-wired to accept visual inputs preattentively ... visual input just goes directly into our brain, sometimes without engaging critical thinking, which means we can form beliefs about states of affairs visually before we've even had a chance to engage critically with what that visual input is really communicating." – Victoria Lemieux, Blockchain@UBC Cluster Lead, Professor of Archival Science at the School of Information, University of British Columbia.

Instances of deepfakes leading to misinformation or fraud have been seen in the past, but the advent of widely available generative AI tools to create the deepfakes and generate content with them escalates the threat posed. In the Global Risks Report 2024, the World Economic Forum ranks misinformation and disinformation as the most severe threat the world faces for the next two years. That's ahead of extreme weather events, social polarization, and cyber insecurity.

Report authors are clear that AI-generated content producing falsified information is the main driver behind the misinformation threat, including deepfakes. "Synthetic content will manipulate individuals, damage economies and fracture societies in numerous ways over the next two years," they write. "New classes of crimes will also proliferate, such as non-consensual deepfake pornography or stock market manipulation" (WEF, 2024).

Cyberattackers can use deepfakes to impersonate decision-makers on audio and video channels, making phishing attacks targeting employees, previously mostly limited to emails, all that more convincing. Or prominent organizations could see their reputations damaged by deepfakes of leaders released into the public realm.

"Deepfakes and the misuse of synthetic content pose a clear, present, and evolving threat to the public across national security, law enforcement, financial, and societal domains." – Department of Homeland Security, 2021

The risk is perhaps greatest in swaying political outcomes, with deepfakes threatening to confuse an electorate by impersonating candidates or elected officials. Aspen Digital is a non-profit organization that seeks to empower people and organizations to be responsible stewards of technology and media, and it has warned about several risks associated with AI and the upcoming US presidential election (2024):

Hyperlocal voter suppression: Bad actors could spread false information to discourage voters in specific communities from casting their ballots.

Language-based influence operations: AI allows for instant translation of text between languages, which can enable the spreading of lies when in the wrong hands.

Deepfaked public figures: As already seen in other elections around the world, public figures can be depicted saying or doing something that they did not.

"DEEPFAKES AND THE MISUSE OF SYNTHETIC CONTENT POSE A CLEAR, PRESENT, AND EVOLVING THREAT TO THE PUBLIC ACROSS NATIONAL SECURITY, LAW ENFORCEMENT, FINANCIAL, AND SOCIETAL DOMAINS."

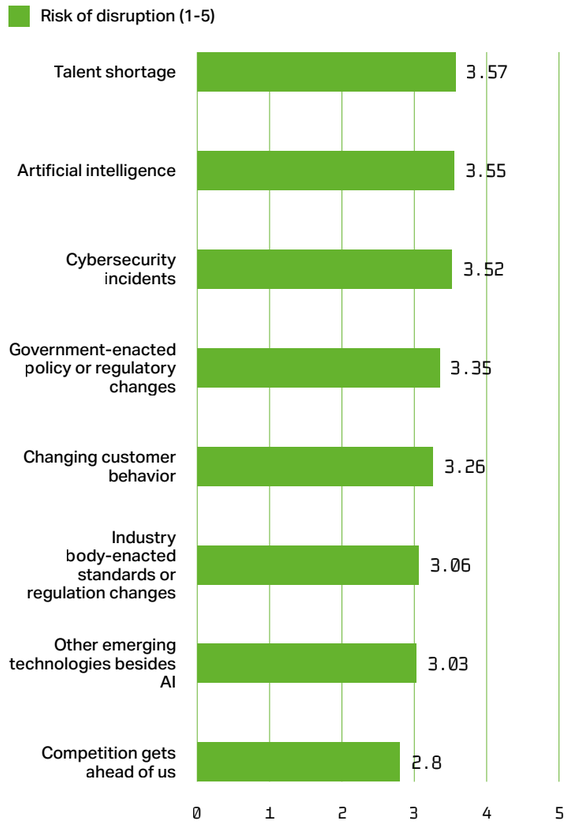
DEPARTMENT OF HOMELAND SECURITY, 2021

AI VIEWED AS A DISRUPTIVE FORCE

The potential of AI to be harnessed by bad actors, while creating new vulnerabilities or pitfalls for organizations to contend with internally, feeds into AI being viewed as an overall disruptive force. IT leaders rank AI as the second most likely factor to disrupt their business in the next 12 months, a close second to the talent shortage. AI ranks ahead of cybersecurity incidents, government-enacted policy or regulatory changes, and changing customer behavior among other factors.

HOW LIKELY IS IT THAT THE FOLLOWING FACTORS WILL DISRUPT YOUR BUSINESS IN THE NEXT 12 MONTHS?

n=697



IT LEADERS WORRY ABOUT DEEPFAKES

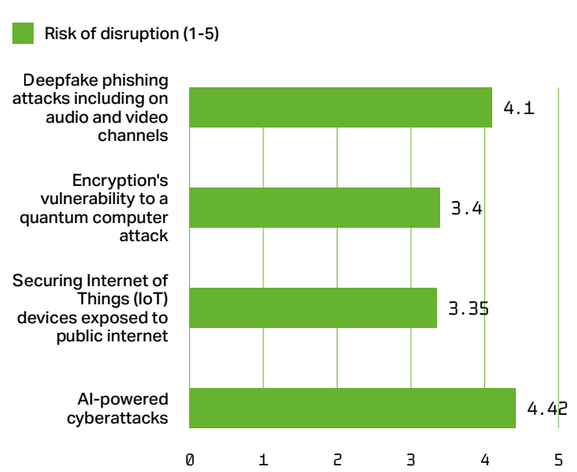
While IT leaders are likely factoring in the disruptive impact of their competition harnessing AI to push them out of the market, the potential for cybercriminals to harness it to cause more direct damage is front of mind.

Our survey respondents rate their concern over AI-powered cyberattacks in general at a 5 out of 5 – as high as possible. Deepfake phishing attempts are also causing concern, rated at 4.5 out of 5 on the concern scale. (When using median scores.) These AI-powered threats are causing more concern than encryption being broken or IoT devices not being secure, among other threats.

New technologies are giving old threats a new dimension. How can organizations respond?

HOW CONCERNED ARE YOU ABOUT THE FOLLOWING EXTERNAL CYBERSECURITY THREATS?

n=155 (security leaders only)



TREND 06 | DEEPFAKE DEFENSE

MITIGATION

Stick to what you know

Some long-tested tactics to defend against malicious actors will still help ward off new attacks powered by AI. It's where most organizations plan to start.

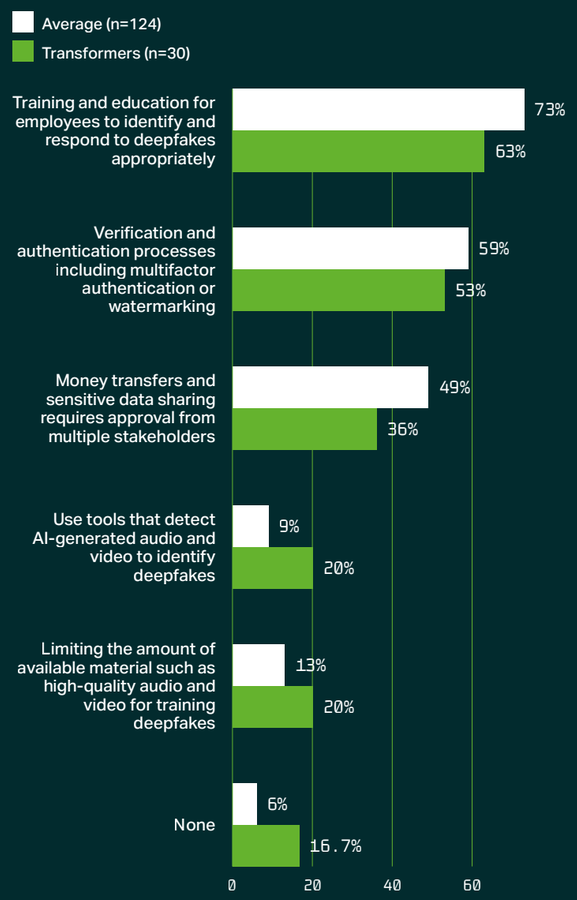
A human-centric approach to cybersecurity has been preached for years to strengthen the weakest link in the cybersecurity chain: people. Too often, it's a worker clicking on a malicious link in an email or falling for a social engineering attack through social media that leads to a data breach. With deepfakes threatening to make those types of attacks even more common and more sophisticated, IT security leaders plan to focus on training and education for employees to identify and respond to deepfakes appropriately. Average IT departments are slightly more likely to prioritize this method than Transformers, saying they will employ the tactic 73% of the time compared to 63% of the time.

Transformers are twice as likely as the Average group to use tools that detect AI-generated audio and video to identify deepfakes, with one in five saying they will do this compared to 9% of the Average. Transformers are also thinking about how to prevent AI deepfakes of their executives in the first place, with 20% saying they will work to limit the amount of available material such as high-quality audio and video for training deepfakes. Only 13% of the Average group is doing this.

"[Even with training, however, it] can be very difficult to dislodge false beliefs that are established through these deepfakes. We can train ourselves. We can become more conscious and more aware. I think we are as a society, but it really is kind of fighting our human nature and our own visual cognitive systems ... it's asking you to be less human in a way, to become more like machines in how we process information. " – Victoria Lemieux, Blockchain@UBC Cluster Lead, Professor of Archival Science at the School of Information, University of British Columbia

Overall, most organizations are relying on employee training and verification and authentication processes, including multifactor authentication or watermarking, as the main tools to protect themselves.

WHAT TACTIC(S) DOES YOUR ORGANIZATION USE TO PROTECT AGAINST DEEPFAKE-POWERED PHISHING ATTACKS INCLUDING PHONE CALLS OR VIDEOCONFERENCE CALLS WHERE AI IS USED TO IMITATE DECISION-MAKERS?



AI BRINGS NEW THREATS THAT REQUIRE NEW RESPONSES

In the future, the new threats of generative AI and the convincing deepfakes it can generate will require a new assortment of preventative measures to make society's information ecosystem more reliable and robust. The range of measures will require organizations to take independent action, cooperate with vendors and industry groups, and follow the best practices and standards developed by regulators.

In some instances, new technology approaches will help defend the world's knowledge exchange from tampering by bad actors. Yet each solution has its weaknesses.

Authentication through blockchain: Blockchain could play a role in verifying the origin of digital content. Blockchain technology creates an immutable digital ledger that is shared among an ecosystem of stakeholders. Its decentralized architecture, with exact copies of the database stored on each individual user's local storage, creates a trusted ecosystem to operate. Information about each user's contributions to the ledger and the content stored are logged, allowing the provenance of information to be tracked. A knowledge ecosystem where content is stored alongside metadata such as hashes that contain timestamps, user identification, and a content signature could help track the origin and integrity of content like videos and photos. This approach would require a shared ecosystem, where both creators and content consumers participate in the blockchain to benefit from its features. However, the approach also only guarantees the provenance of the content, not its veracity – you may know where the image is coming from, but you may not know if it represents what really happened, that is to say, even a known source can falsely guarantee a deepfake under certain circumstances. (Interview with Victoria Lemieux)

AI-powered detection tools or watermarking: Tools to detect AI-generated content on the user side can be released by either AI creators or others in the community who want to help prevent misinformation with AI. Such solutions have become common in the education space, where professors and teachers want to ensure their students are writing their own essays instead of prompting ChatGPT to do so.

These tools can be issued by a manufacturer of an AI generation tool. In this case they are often paired with a watermarking technique, where the AI vendor provides extra information beyond the content generated that would help tools easily identify it as AI generated. This approach could be integrated into social media platforms and news publisher websites to help content creators and users quickly separate AI-generated content from authentic content created by people.

Detection tools released by third parties tend to generate a confidence score about the probability that content is AI generated rather than provide a binary yes/no answer. While some of these tools have been put into regular use, there are several shortcomings to the approach:

AI creators are holding back: OpenAI has a tool that can reliably detect when its models have been used to generate writing but is reluctant to release it for fear it would discourage users. OpenAI even conducted a survey among users to see if they'd be discouraged from using the service if a detection tool was released and found that one-third would be turned off. The tool requires OpenAI apply a watermarking method to its ChatGPT tool, slightly altering the word fragment (or token) selected to appear in a sentence in a way that would be unnoticeable to people but result in detection by the tool 99.9% of the time. (The Wall Street Journal, August 2024)

Watermarks can be removed: If an AI tool is available as an open-source model, or if its proprietary model details are leaked, bad actors can remove or alter the watermarking methods and render tools ineffective.

Watermarks can be added: Just as easily as a known watermark can be stripped, it could be added to real content in an attempt to make it seem like real media was generated by AI. Bad actors could employ this tactic to seed doubt about the veracity of real content. (NBC News, 2024)

It's an arms race: Similar to the cat and mouse game that hackers play with cybersecurity providers, those creating models and external players providing ways to detect them will constantly be chasing each other. AI creators will change the way their model behaves often, potentially making detection tools less effective until they are updated to counter the model. (Interview with Victoria Lemieux)

Content authenticity: Instead of adding watermarks to AI-generated images, another approach could see content digitally signed by the creator. It functions much like in medieval times when the King's signet ring was used to leave an impression in a wax seal on an envelope, says Lemieux. This approach ultimately depends on verification by signature of the digital signing method itself. However, a letter with the King's seal on it – or a digital signature – could still have been one created by an impostor with a fraudulent ring or its contemporary equivalent, or it could have been intercepted en route and the message altered. Modern technology approaches may make this sort of tampering more difficult than in medieval times but not impossible.

TREND 05 | AI AVATARS

EXAMPLES

In search of a robust deepfake defense

Despite the shortcomings of individual approaches, some are pursuing efforts to implement them in hopes they could take part in a multi-faceted approach to protect society's chain of knowledge creation. Individual organizations will have to think about their part in the ecosystem and determine where they want to take action to add trust to their own content distributed to employees or the wider public. They'll also have to track vendor and regulator initiatives seeking to protect against misinformation to be aware of what content should be trusted online, learn how employees can fend off sophisticated AI-powered cyberattacks, and determine what measures should be applied to their own content creation.

Some examples of specific solutions being pursued:

SWEAR WANTS TO UNDERPIN TRUSTED VIDEO ON THE INTERNET:

SWEAR Inc. offers technology that brings blockchain-based authenticity to digital media assets. SWEAR's technology demonstration is powered by an iPhone app that allows users to take record videos with unique hashed signatures in real time. The technology could be integrated with Android smartphones or embedded in other recording devices such as cameras. The video content is embedded with a "cryptographic fingerprint to map every frame, pixel, sound bite, and layers of attribution data," according to SWEAR's solution brief. The data includes information on which user shot the footage or edited the footage and when it was done, among other data points. The hash created is stored on a blockchain and the digital media assets are stored separately in a secure environment. Users are shown a confidence score indicating how likely it is that the content is authentic.

"We're putting on our tinfoil hats and asking how can you try to fake this? We try to capture as much information as we can, and we watermark it directly into the video in real time." – SWEAR CEO Jason Crawforth

According to founder and CEO Jason Crawforth, the mission of SWEAR is not to create its own platform where users will exchange authentically certified videos. "Let's be honest, we're an acquisition target," he says. "We wanted to show Apple and Google that we have the ability to use this technology should we integrate it directly into the OS level." Or social media platforms seeking a solution for preserving user trust could consider implementing it, he adds.

While SWEAR is blockchain agnostic and could use different options available, its technology demo that includes an iPhone app is relying on Hyperledger. The permissioned distributed ledger is recognized by large technology vendors and works efficiently, Crawforth says. SWEAR was awarded the 2024 Judges' Choice Award by the Security Industry Association. (Interview with Jason Crawforth)

USING METHODS OF THE PAST ON THE CONTENT OF THE FUTURE:

Archival sciences provide a toolset that practitioners use to verify the authenticity of recovered historical documents. That could provide some insight on how to separate AI-generated misinformation from real content, according to Victoria Lemieux. She is collaborating with researchers from Carleton University on a prototype solution that users can apply to assess content's authenticity.

> "EPISTEMIC SECURITY IS TRYING TO FIGURE OUT WHAT TO DO WHEN WE REALIZE WE DISAGREE ABOUT THE FACTS. WHEN WE HAVE SUCH DIVISIONS IN SOCIETY, WE NEED TO HARMONIZE AROUND A CONSENSUS ... A SHARED TRUTH. A SOCIETY THAT DOESN'T HAVE A SHARED TRUTH IS GOING TO BE DIVIDED."
>
> VICTORIA LEMIEUX,
> BLOCKCHAIN@UBC CLUSTER LEAD AND PROFESSOR OF ARCHIVAL SCIENCE AT THE SCHOOL OF INFORMATION, UNIVERSITY OF BRITISH COLUMBIA.

"Epistemic security is trying to figure out what to do when we realize we disagree about the facts. When we have such divisions in society, we need to harmonize around a consensus ... a shared truth. A society that doesn't have a shared truth is going to be divided." – Victoria Lemieux, Blockchain@UBC Cluster Lead and Professor of Archival Science at the School of Information, University of British Columbia.

THE WHITE HOUSE PLANS TO CRYPTOGRAPHICALLY SIGN ITS COMMUNICATIONS:

After reports of a deepfake of President Joe Biden's voice made robocalls discouraging voters during a New Hampshire primary election, the threat of AI-generated mimics of elected leaders became clear. The White House is responding by planning cryptographic verification of communications from text statements to videos. This would allow users to verify the source of content that looks like it might come from the President. (Cybernews, 2024)

CONTENT AUTHENTICITY INITIATIVE BUILDS A COALITION FOR CONTENT CREDENTIALS:

Founded by **Adobe** in 2019, the CAI has grown to include 2,000 media and technology companies committed to using open-source tools to verifiably record the provenance of any digital media, even if made with generative AI. The coalition leverages the technical standards created by the Coalition for Content Provenance and Authenticity (C2PA) and seeks to build a community around the movement. Technology members include camera and chip manufacturers working to embed verification methods directly into their tools. (CAI)

/ imagine
a holographic salesperson delivering their sales pitch, smiling, charming, there are different voice prints superimposed over the image to indicate a range of voices --style raw
--v 6.0 --ar 17:11

WHAT'S NEXT?

1

Audio-based AI agents will outpace visual AI agents in 2026, with clear applications in customer support and entertainment.

2

More than 90% of organizations will have a chatbot agent for employees deployed by the end of 2026.

3

Agentic AI will become more popular in 2025. Systems involving multiple LLMs that excel at different types of tasks will be coordinated in this approach that seeks to take a user intent and operationalize it from start to finish, completing actions across multiple steps to complete more complex tasks involving different applications, data, and processes.

4

A new ecosystem of solutions will grow from the need to sort out what's real from what's fake on the internet. Multiple solutions will need to combine to solve different aspects of the problem, to help determine a material's veracity, provenance, and integrity. Both content creators and consumers will need to participate in the ecosystem to create a reliable chain of information truth.

CONCLUSION

Place your bets

In the years following The Manhattan Project and his work helping to create the Monte Carlo simulation method, scientist John von Neumann continued on to receive many accolades as a math pioneer. He solved some of society's greatest problems, including some related to climate change. He even contemplated the concept of Exponential IT.

Neumann described "the ever-accelerating progress of technology and changes in the mode of human life, which gives the appearance of approaching some essential singularity in the history of the race beyond which human affairs, as we know them, could not continue."

Neumann's pondering of a future that is incompatible with current everyday life isn't unique. At a time of rapid change and growing uncertainty about what the future holds, many are suffering from a case of "future shock" and feeling as if even contemporary technology advances have profound implications for humanity's place in the world. Consider the AI observers that caution about reaching a singularity where AI achieves its own agency and exits human control. The pressure to keep pace with emerging technology is particularly pronounced among IT leaders who feel pressured to follow that sharp turn up the exponential curve.

If you find yourself feeling the effects of future shock, don't hesitate. Instead, take the lessons from Neumann's early work on the Monte Carlo method:

THE FUTURE ISN'T DETERMINED, BUT THERE ARE MANY POTENTIAL SCENARIOS THAT CAN UNFOLD. IF YOU WANT TO WIN, YOU'LL HAVE TO PLACE YOUR BETS DOWN AND INVEST IN THE RIGHT SOLUTIONS. IF YOU DO AND YOU'RE LUCKY, EXPONENTIAL REWARDS MIGHT JUST BE IN THE CARDS.

EXPERT CONTRIBUTORS

OVERALL PLANNING

David Glazer,
Strategic Advisor and Futurist Speaker

Douglas Heintzman,
Chief Catalyst, Blockchain Research Institute

EXPONENTIAL AI

Alirezza Sharifi,
Co-Founder of Nubinary

Liam Nediger,
CTO, Info-Tech Research Group

Mark Montgomery,
Founder and CEO, Kyield

Marinela Profi,
Strategic AI Advisor, SAS

PRE-QUANTUM FOUNDATIONS

Kathrin Spendier
Technical Prize Director, XPRIZE Quantum

Marieke Hood,
Executive Director Impact Translator, GESDA

Gaylen Bennett,
Offering Manager, IBM Quantum Industry & Technical Services

Imed Othmani,
Industry Partner, IBM Quantum Industry & Technical Services

Ian Pratt,
Global Head of Security for Personal Systems at HP Inc.

DIGITAL HUMANS

Jay O'Connor,
CEO, Voices.com

Jason Crawforth,
CEO, SWEAR

Victoria Lemieux,
Blockchain@UBC Cluster Lead,
Professor of Archival Science at the School of Information,
University of British Columbia

BIBLIOGRAPHY

OVERALL

"Monte Carlo Simulation – History." Virginia Tech, n.d. Retrieved from The Wayback Machine, 25 Oct. 2020 capture.

"Sense-Making Futures: A Crisis of Certainty." Policy Horizons Canada, Government of Canada, 16 April 2024.

EXPONENTIAL AI

Bousquette, Isabelle. "AI Work Assistants Need a Lot of Handholding." The Wall Street Journal, 25 June 2024. Accessed 27 June 2024.

Bousquette, Isabelle. "At Moderna, OpenAI's GPTs Are Changing Almost Everything." The Wall Street Journal, 24 April 2024.

Bousquette, Isabelle. "Goldman Sachs Deploys Its First Generative AI Tool Across the Firm." Wall Street Journal, 27 June 2024.

Gartenberg, Chaim. "What Is a Long Context Window?" The Keyword, Google, 16 Feb. 2024.

"GenAI Market Research: 80% of Leaders Concerned about Data Privacy and Security." SAS, 17 April 2024. Accessed 10 May 2024.

He, Xu Owen. "Mixture of a Million Experts." arXiv, 4 July 2024, arXiv:2407.04153.

Johnston, Lisa. "How Mars Is Using Generative AI to Accelerate Product Development and Personalization." Consumer Goods Technology, 13 June 2024. Accessed 20 June 2024.

Lamarre, Eric, et al. "The Value of Digital Transformation." Harvard Business Review, 31 July 2023. Accessed 20 June 2024.

Lu, Yiwen. "Digital Media Outlets Sue OpenAI for Copyright Infringement." The New York Times, 28 Feb. 2024.

Mandell, Sharon. "FOMO vs. FOMU: Working Through Real, Valid Fears About Enterprise AI Adoption." Official Juniper Networks Blogs, 13 Feb. 2024.

Marinotti, Joao. "Commentary: Could a Court Really Order the Destruction of ChatGPT?" CNA, 29 Jan. 2024. Accessed 26 June 2024.

Mickle, Tripp, et al. "Apple Will Revamp Siri to Catch Up to Its Chatbot Competitors." The New York Times, 10 May 2024.

Miller, Ron. "In Spite of Hype, Many Companies Are Moving Cautiously When It Comes to Generative AI." TechCrunch, 19 June 2024.

Montgomery, Mark. "What Is AI Sovereignty? And Why It Should Be the Highest Priority." LinkedIn, 14 May 2024. Accessed 21 May 2024.

Montgomery, Mark. "What Is an EAI OS?" LinkedIn, 13 July 2023.

Pearson, Jordan. "What the RIAA Lawsuits against Udio and Suno Mean for AI and Copyright." The Verge, 26 June 2024. Accessed 26 June 2024.

Pines, Matthew. "PinnacleOne ExecBrief | Digital Sovereignty and Splinternets in Cloud, AI & Space." SentinelOne, 6 May 2024.

Rikap, Cecilia. "Dynamics of Corporate Governance Beyond Ownership in AI." Common Wealth, 15 May 2024. Accessed 29 May 2024.

Sagan, Aleksandra. "Canadian Tire's Artificial Intelligence Push Gets Real." The Logic, 1 Nov. 2023.

Sharp, Andrew. "Secure Your Generative AI Applications on AWS, Azure, and GCP." Info-Tech Research Group, 1 May 2024. Accessed 22 May 2024.

Toneguzzi, Mario. "Canadian Tire Launches AI Shopping Assistant and Humanoid Robots to Enhance Customer Service and Operations [Interview]." Retail Insider, 12 May 2024. Accessed 8 July 2024.

PRE-QUANTUM FOUNDATIONS

"2023 Quantum Threat Timeline Report." Global Risk Institute, 22 Dec. 2023. Accessed 15 May 2024.

Ahmad, Suleman. "Cloudflare Now Uses Post-Quantum Cryptography to Talk to Your Origin Server." Cloudflare, 29 March 2023.

Apple SEAR. "iMessage with PQ3: The New State of the Art in Quantum-Secure Messaging at Scale - Apple Security Research." Apple Security Research, 21 Feb. 2024. Accessed 1 Aug. 2024.

Coker, James. "HSBC Joins Quantum-Secure Network." Infosecurity Magazine, 7 July 2023.

Coker, James. "NIST Publishes Draft Post-Quantum Cryptography Standards." Infosecurity Magazine, 24 Aug. 2023.

Dargan, James. "13 Quantum Cloud Computing Software Companies in 2024." The Quantum Insider, 3 May 2022.

Dargan, James. "Quantum Computing Companies: A Full 2024 List." The Quantum Insider, 29 Dec. 2023.

Delgado, Alain, et al. "Simulating Key Properties of Lithium-Ion Batteries with a Fault-Tolerant Quantum Computer." Physical Review A, vol. 106, no. 3, Sept. 2022, p. 032428. arXiv.org.

"Falcon." https://falcon-sign.info/

Gambetta, Jay. "The Hardware and Software for the Era of Quantum Utility Is Here." IBM Quantum Computing Blog, IBM, 4 Dec. 2023.

Gosselink, Brigitte Hoyer. "Google, GESDA and XPRIZE Launch New Competition in Quantum Applications." The Keyword, Google, 4 March 2024.

"HSBC and Quantum." HSBC, n.d. Accessed 13 May 2024.

Hughs-Castleberry, Kenna. "Zapata Computing Finds That 71% of Quantum-Adopting Global Enterprises Dedicated at Least $1M to Quantum Computing Initiatives in a New Report." Inside Quantum Technology, 11 Jan. 2023.

"IBM-Developed Algorithms Announced as NIST's First Published Post-Quantum Cryptography Standards." IBM Newsroom, 13 Aug. 2024. Accessed August 14, 2024.

"IBM Quantum Computer Demonstrates Next Step Towards Moving Beyond Classical Supercomputing." IBM Newsroom, 14 June 2023. Accessed 27 May 2024.

Kaur, Maninder. "Overview of Quantum Initiatives Worldwide 2023." Qureca, 19 July 2023.

Kerstens, Rob. "Introducing BenchQ, the Result of Our Work With DARPA." Zapata AI, 11 Dec. 2023.

Krause, Reinhardt. "After Artificial Intelligence, Quantum Computing Could Be The Next Big Thing." Investor's Business Daily, 16 June 2023.

Moody, Dustin. "Are We There Yet? An Update on the NIST PQC Standardization Project." NIST, Fifth PQC Standardization Conference, 10 April 2024.

Mosca, Michele. "The Race Is on - Quantum Threat Timeline Primer." Global Risk Institute, 14 Dec. 2023.

"NIST Releases First 3 Finalized Post-Quantum Encryption Standards." NIST, 13 August 2024.

"NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers." NIST, 24 Aug. 2023.

"Our Projects | Discovery Accelerator." Cleveland Clinic, n.d. Accessed 29 July 2024.

Pereira, Brian. "IBM Primes Its Quantum Computers for Business Applications." CIO.Inc, 3 May 2024.

"Post-Quantum Cryptography." Homeland Security, 4 Oct. 2022. Accessed 15 May 2024.

"Post-Quantum Cryptography: CISA, NIST, and NSA Recommend How to Prepare Now." National Security Agency/Central Security Service, 21 Aug. 2023. Accessed 13 May 2024.

"qBraid Lab: A Preferred Notebook Environment for Former IBM Quantum Lab Users." qBraid, 3 June 2024. Accessed 7 June 2024.

"Q-CTRL Transforms Quantum Advantage Outlook, Breaking Previous Records for Optimization Problems and Outperforming Competitive Technologies." Q-CTRL, 5 June 2024. Accessed 20 June 2024.

BIBLIOGRAPHY

PRE-QUANTUM FOUNDATIONS (CONT'D)

"Quantum-Readiness: Migration to Post-Quantum Cryptography." CISA, NIST, 21 Aug. 2023. Accessed 13 May 2024.

Rep. Khanna, Ro [D-CA-17]. "Text - H.R.7535 - 117th Congress (2021-2022): Quantum Computing Cybersecurity Preparedness Act." 117th Congress, 21 Dec. 2022,

Sadyiko, Alexey. "Apple Has Released a New Way to Protect Instant Messaging in iMessage." Kaspersky, 23 Feb. 2024.

Schirber, Michael. "A Moving Target for Quantum Advantage." Physics, vol. 17, 23 Jan. 2024, p. 13.

Siegel, Ethan. "Quantum Supremacy Explained." Big Think, 30 Aug. 2023.

"SK Telecom and Thales Collaborate on Post-Quantum Cryptography to Enhance Users' Protection on 5G Network." Thales Group, 19 Dec. 2023.

Soltys, Douglas. "Xanadu's Christian Weedbrook Is Raising Another $200 Million to Build a Quantum Data Centre." BetaKit, 24 May 2024.

Soni, Paul, and Bobby Henninger. "The Journey to Computing's 'Holy Grail' Is Gaining Momentum - KPMG Global." KPMG, 29 Nov. 2022.

Stockpole, Beth. "Quantum Computing: What Leaders Need to Know Now." MIT Sloan, 23 May 2024.

"Toshiba, HSBC Launch AI-Protected Quantum FX Trading." Toshiba Quantum Technology, 15 March 2024. Accessed 13 May 2024.

Wong, Thomas. "NQIAC Report on Renewing the National Quantum Initiative." National Quantum Initiative, 2 June 2023.

DIGITAL HUMANS

"2024 Audio Trends for Voice Actors." Voices, 4 Jan. 2024. Accessed 12 June 2024.

"2024 Client Trends Report." Voices, 6 Dec. 2023. Accessed 12 June 2024.

"AI Voice Generator Market Size, Share | CAGR of 15.4%." Market.Us, Nov. 2023. Accessed 1 Aug. 2024.

"Bank ABC's AI-Powered Digital Employee 'Fatema' Is the World's First Digital DNA (TM) Human." Bank ABC, 11 Sept. 2019. Accessed 2 Aug. 2024.

"Conversational AI for IT Services and Employee Experiences - Solutions." Amelia, n.d. Accessed 7 June 2024.

Deloss, John. "William Shatner Has Become an Interactive AI You Can Chat With." ScreenRant, 11 Oct. 2021.

"Digital Einstein: A genius for the AI era." UneeQ and the Hebrew University of Jerusalem, n.d. Accessed 7 June 2024.

Eaton, Kit. "Is It a Person, or an AI Chatbot? Tests Say Maybe We Can't Tell." Inc., 24 June 2024.

Edwards, Benj. "Zoom CEO Envisions AI Deepfakes Attending Meetings in Your Place." Ars Technica, 4 June 2024

"Global Risks Report 2024." World Economic Forum, 10 Jan. 2024. Accessed 2 Aug. 2024.

Hoffman-Andrews, Jacob. "AI Watermarking Won't Curb Disinformation." Electronic Frontier Foundation, 5 Jan. 2024.

"How It Works." Content Authenticity Initiative (CAI), n.d. Accessed 6 Aug. 2024.

"How Many People Use Google? Statistics & Facts (2024)." SEO.ai, 24 April 2024. Accessed 1 Aug. 2024.

"Increasing Threat of Deepfake Identities." U.S. Department of Homeland Security, 11 August 2021.

Kuhn, Daniel. "US Defense Department to Develop Blockchain Cybersecurity Shield." CoinDesk, 29 July 2019.

Kulkarni, Neha Pradhan. "How Ericsson Uses Digital Humans to Drive Business Growth." Spiceworks Inc, 18 Jan. 2023. Accessed 7 June 2024.

Latkowski, Tom. "AI Risks Facing the 2024 US Elections." A.I. Elections Initiative, Aspen Digital, 17 June 2024. Accessed 18 June 2024.

Lukan, Emma. "Digital Humans Are Here — and They're Changing Everything." Synthesia, 13 June 2024. Accessed 7 June 2024.

"LynkAI - Powering the next Generation of Connected Experiences." Ericsson.com, n.d. Accessed 7 June 2024.

Magramo, Kathleen. "British Engineering Giant Arup Revealed as $25 Million Deepfake Scam Victim." CNN, 17 May 2024.

Meikkila, Melissa. "Three Ways We Can Fight Deepfake Porn." MIT Technology Review, 29 Jan. 2024. Accessed 6 Aug. 2024.

"MetaHuman | Realistic Person Creator." Unreal Engine, Epic Games Inc., 2024.

Metz, Cade, and Tiffany Hsu. "OpenAI Releases 'Deepfake' Detector to Disinformation Researchers." The New York Times, 7 May 2024.

Mickle, Tripp, et al. "Apple Will Revamp Siri to Catch Up to Its Chatbot Competitors." The New York Times, 10 May 2024.

"Misinformation, Polarization Among Top Short-Term Risks: WEF Report." IISD SDG Knowledge Hub, 19 Jan. 2024. Accessed 13 June 2024.

Parsani, Puran. "Case Study: The AI Behind Virtual Influencer Lil Miquela." Cut The SaaS, 22 Nov. 2023. Accessed 2 Aug. 2024.

Radauskas, Gintaras. "White House Will Fight Deepfakes with Cryptographic Verification." Cybernews, 12 Feb. 2024.

Robins-Early, Nick. "CEO of World's Biggest Ad Firm Targeted by Deepfake Scam." The Guardian, 10 May 2024.

Seetharaman, Deepa, and Matt Barnum. "There's a Tool to Catch Students Cheating With ChatGPT. OpenAI Hasn't Released It." The Wall Street Journal, 4 Aug. 2024.

"Sense-Making Futures: A Crisis of Certainty." Policy Horizons Canada, Government of Canada, 16 April 2024.

Seymour, Mike, et al. "AI with a Human Face." Harvard Business Review, 1 March 2023.

Sundaram, Ashok. "Digital Humans: Providing Personalized Experiences at Scale." Cognizant, 18 March 2024. Accessed 7 June 2024.

Tenbarge, Kat. "Why AI Watermarks Miss the Mark in Preventing Misinformation." NBC News, 19 March 2024.

"Using the Blockchain to Combat Disinformation." Coinbase Institute, 21 June 2023. Accessed 6 May 2024.

"Voices Gives Emotion to AI Voice with the Launch of Its New AI Studio." Voices, 6 June 2024. Accessed 12 June 2024.

Zink, Kevin. "Top 10 Microsoft Copilot Use Cases for Enterprises." US Cloud, 29 April 2024.

INFO~TECH
RESEARCH GROUP

North America 1-888-670-8889

United Kingdom 0808 175 3350

Australia 1800 242 692

International +1-519-432-3550

INFOTECH.COM