ITC INFOTECH

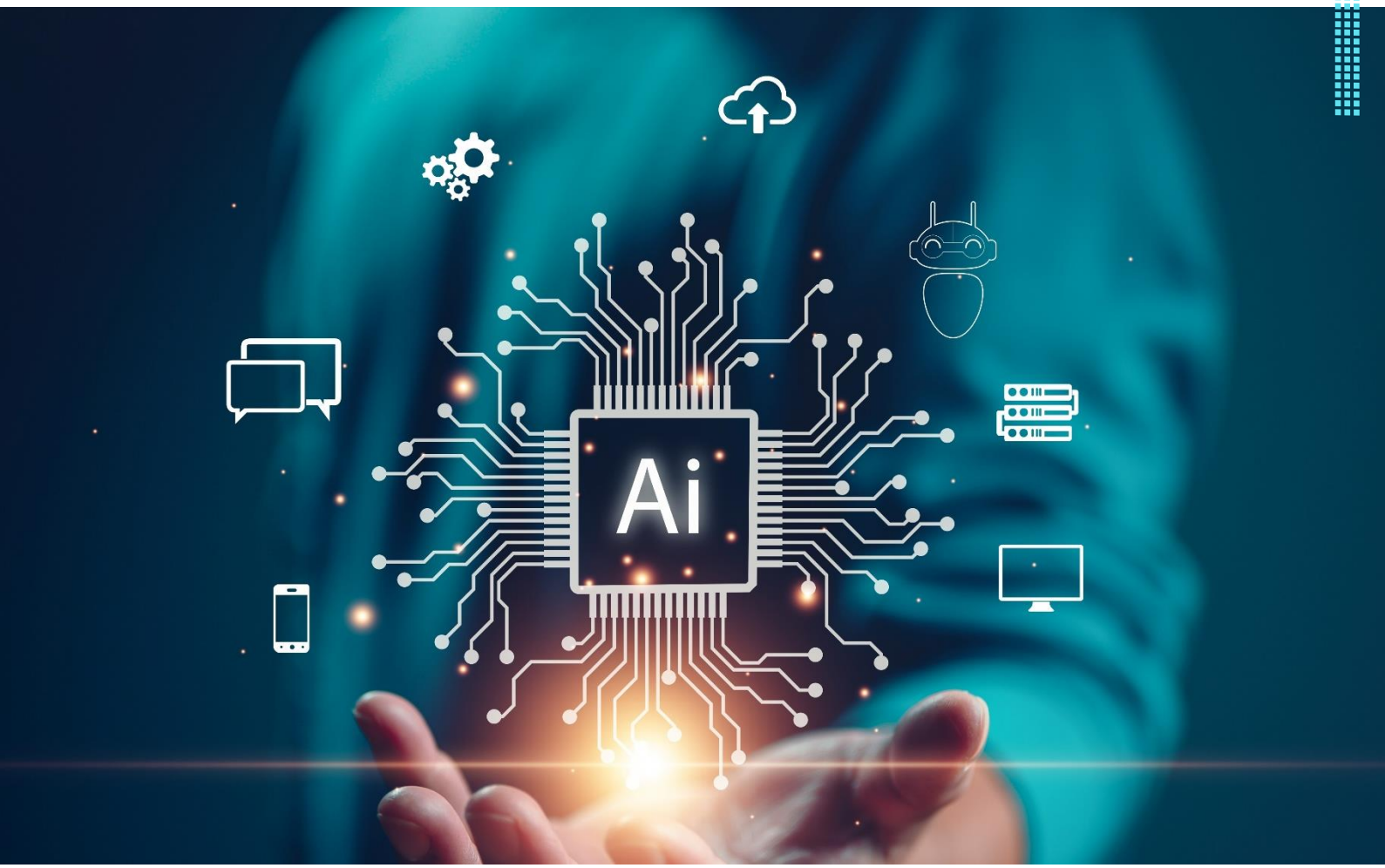
Business-friendly Solutions

Getting Behind Generative AI While Avoiding the Pitfalls

Introduction

Business leaders have been very receptive to Generative AI. Reason: As a system of intelligence, Generative AI helps analyze information and create new applications and artifacts more quickly and efficiently. The fast-moving technology promises to change how businesses are structured and run. However, organizations are not certain if they are adding to the digital complexity of their business and increasing technology risks by adopting Generative AI.

Generative AI does not require users to understand the technology or how to use it to extract insights from data. Instead, it uses natural language that anyone can use to interact with complex systems, producing answers and creating ready-to-use reports, code, bots, applications, text, images, audio, and video. Used correctly, it is a rapid enabler of business transformation.



Some common applications enabled by Generative AI

Customer Assistance Bots

Bots that listen to and understand customer queries and needs to answer questions, provide assistance, and recommend products and services.

Coworker Bots

Bots that have specialized capabilities that function as co-workers, helping employees become more productive.

Creative Content

Helping create product descriptions, reports, fresh marketing, sales, training, and educational content in the form of text, images, audio, and video that can be personalized without the need to be a trained designer or content producer.

Data Analytics

Using simple, natural language queries, lets everyone have access to quality insights from their internal and external, structured and unstructured data using models specific to their roles and industry.

Data Augmentation

Creating synthetic data to increase the number of data points and improve the diversity of the data necessary to train AI models.

Coding for Apps

Faster deployment of products at lower costs.

Testing and Debugging

Creating new test cases and simulating scenarios to improve the quality of the code.

Security Management

Monitoring and management, which includes automated identification, investigation and response to threats for improved asset protection and compliance.

Business Automation

Streamlining workflows and automating repetitive tasks to achieve higher process accuracy, adding to capacity, and lowering costs

Generative AI has wide applications in areas that businesses across industries want to optimize. It has also found quick acceptance because it is a layer on top of existing technology investments. Businesses do not have to rip and replace anything. The only challenge is integrating Generative AI with existing systems as quickly as possible to extract more from enterprise data. But businesses could be hesitant. In the past, they have not found AI integration easy, nor has the ROI been as quick as promised.

When things go wrong

It is easy to see that the upside of Generative AI is significant. Enterprises will apply Generative AI wherever possible—and as quickly as possible. However, given the challenges and ethical considerations involved with Generative AI, things will, and can, go wrong quickly. Here are three recent examples from real life:

- In 2023, an employee of one of the older airlines in the US filed a case for injuries he had sustained in 2019. His attorney used ChatGPT to find prior cases to support the case. The court examined the evidence submitted by the lawyer and concluded that the documents were filled with bogus judicial decisions, bogus quotes, and bogus internal citations. The lawyer was fined, and the lawsuit was dismissed. The misleading content provided by ChatGPT had let down the lawyer. The incident, a result of poor AI integration, is not isolated.
- A global airline has had to pay for its chatbot that lied to a passenger. This is an example of business transformation gone wrong at the hands of AI.
- Researchers found that deep learning models used to diagnose the COVID-19 virus were not fit for clinical use.

In one model, the training data set used scans from patients who were standing up or lying down. The patients who were lying down were more likely to be ill, and the model learned to assess the risk of the virus based on the position of the person scanned.

What this signals is elementary: We need to be cautious, even perhaps slow down, and apply technology with greater prudence, fostering a sense of responsibility and thoughtfulness in our actions. At no point should AI implementations increase technology risk.

AI vs. Digital Transformation

Over the years, businesses have embraced Digital Transformation and have come to understand it well. Although AI is closely intertwined with Digital Transformation, it is different. The two are distinct concepts within the technology and business landscape.

AI

AI mimics or simulates human intelligence. It uses algorithms with technologies like machine learning, deep learning, natural language processing, and computer vision. Businesses have used AI primarily to enhance decision-making, automate processes such as accounting, customer servicing, recruitment, and inventory management, and enable capabilities such as predictive analytics and personalized experiences.

Digital Transformation

Digital Transformation converts assets, processes, products, and operations into digital format and leverages computer-based technologies to change existing business functions or create new ways to manage them. Digital Transformation improves performance, optimizes operations, enhances customer experience, and creates new sources of value through technologies like mobile, cloud computing, e-commerce platforms, and big data analytics.

[1]In one model, the training data set used scans from patients who were standing up or lying down. The patients who were lying down were more likely to be ill, and the model learned to assess the risk of the virus based on the position of the person scanned.

Relationship

AI is an accelerator and enhancer for Digital Transformation initiatives. It automates tasks, analyzes data for insights, and optimizes processes. AI carries a distinct flavor of automation but is different because, unlike automation, it can learn from new information and self-correct. AI allows businesses to enhance operational efficiency, improve customer engagement, innovate, and respond faster to market trends by leveraging digital assets for speed, scale, and accuracy.

Key Differences

AI technologies are integral components of Digital Transformation efforts. While AI focuses on creating intelligent systems, Digital Transformation encompasses a broader strategic shift toward leveraging digital technologies, analytics, and automation for business improvement.

Growing concerns around the complexity of technology

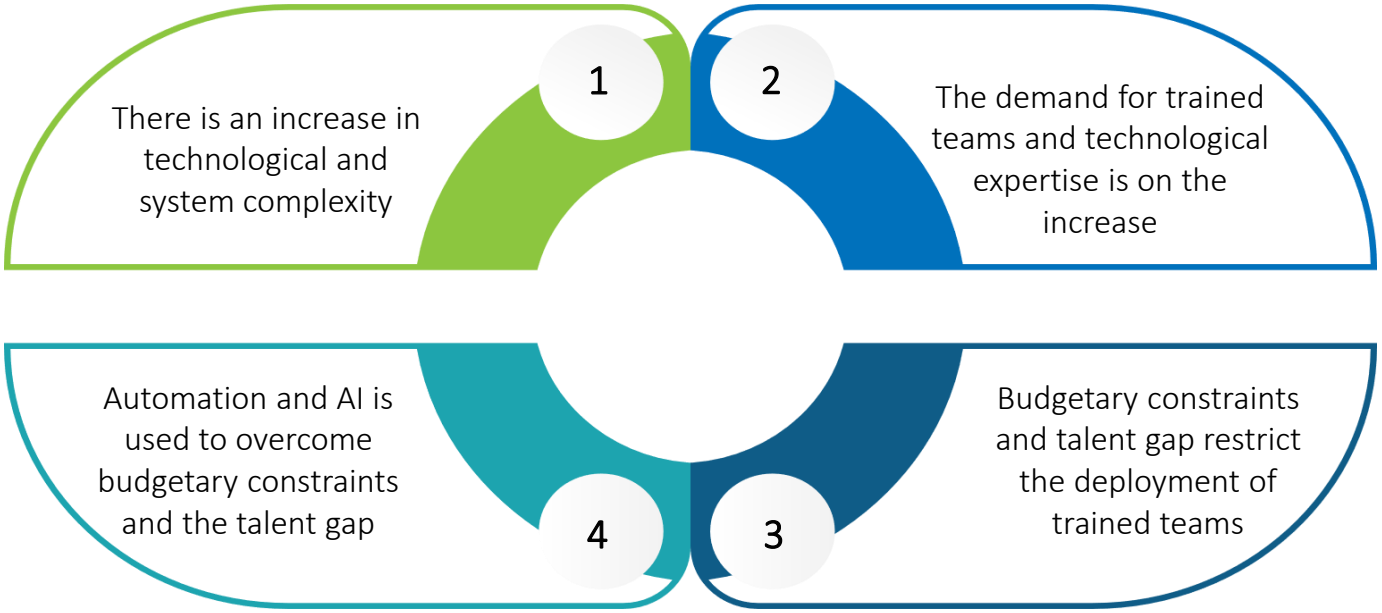
As technologies such as data sciences, deep learning, and AI make their way into businesses, the scale of complexity grows in proportion. Businesses must, therefore, practice a degree of caution. A revolution is happening in technology—especially with the arrival of Generative AI—that is too swift to grasp fully:

- On-prem infrastructure is moving to the cloud, exposing enterprises to complex environments and ecosystems
- A new range of endpoints is coming into play as workloads move into the cloud
- The heterogeneity of cloud systems is becoming a challenge in terms of management, security, governance, and costs
- Standardization is becoming difficult as businesses want to retrofit common security, governance, and management protocols to the emerging chaotic and cluttered technology landscape

In this scenario, the chances of making an error are a hundredfold higher than when distributed computing was taking root. The very heterogeneity of cloud systems, which makes them an attractive business and technological option, is becoming a challenge. As an example, CloudOps is experiencing distress as complex combinations of technology stacks, interfaces, workloads, VMs, platforms, and tools land in their laps.

There was a time when the number of SecOps experts working on a few hundred virtual on-premise servers using two or three platforms (Windows NT, etc.) could be easily counted on the fingers of a single hand. Between them, they managed perhaps two dozen databases (spread across Oracle, MongoDB, PostgreSQL). Today, the same SecOps team manages double the number of virtual servers across different cloud ecosystems and twice the number of purpose-built databases. Since it is difficult to manage this sprawl, the number of members in the SecOps team must increase. However, budget constraints and a talent gap restrict team size. These teams are, therefore, being forced to press automation and AI into service—opening a new Pandora's Box of complexity!

The cycle of technological and digital complexity



Cloud security is a significant concern. With multi-cloud usage, security threats extend to devices, users, and applications. Additionally, with containers and serverless computers, security is becoming the responsibility of developers, turning errors into a more significant problem. The trick is to understand what needs to be automated. Should automation be applied to security in the CI/CD process? In vulnerability scanning? Configuration? Drift management? Compliance management? Infra as code? Container deployment? Incident response? Reporting? And, most importantly, where should it be applied without increasing technology risk?

Modern digital systems also use and generate a vast amount of data. Where is this data coming from? Where does it go? How and where is it stored? Who has access to it? What is the data being used for? On platforms like Azure, it is easy to use data to auto-spin Virtual Machines (VMs) up and down to keep costs down. However, the data generated by cloud ecosystems can be compromised or misused.

Health organizations, for example, share data to ensure patients' treatment is faster when they return. Data generated by applications such as from e-commerce sites, social media, mobile payment systems, and media consumption can be shared with technology companies to predict voter interests during election times. Data from applications that use facial scans to facilitate transactions and access facilities can easily be misused or compromised if stored poorly.

The amount of personal data generated in transport, airlines, retail, and hospitality is enormous. The systems that need to share this data are complex, spread across diverse entities, and need to be better integrated. These ecosystems are expanding in an uncontrolled mode. For example, transport systems share data with fleet owners, vehicle operators, manufacturers/business/cargo owners, warehouses, courier companies, security systems, banking systems, private and government toll collection systems, state and law enforcement agencies, and government visa and emigration systems. The rules and policies that govern these ecosystems are disparate, fragmented, and sometimes mismatched. They are not adequate for protecting the data. In such instances, the threat of data leaks and breaches outweigh the benefits of automation and AI.

Five rules to apply for optimal returns from technology investments

- Stay cautious, apply technology (Generative AI, cloud, data lake, automation, etc.) prudently by identifying the right use cases
- Develop AI-driven solutions to address complex challenges, emphasizing accurate risk assessment and informed decision-making through quantifying uncertainties and probabilities
- Master AI techniques and integrate them with other advanced technologies to effectively tackle complex problems – apply this approach to processes across the business
- Think through the strategy, use responsible processes, leverage ethically sourced data, and pay more attention to security audits
- Strategically prioritize these techniques and solutions based on their relevance and potential impact

Those who have seen security audits conducted firsthand know how little the audits can mean. About 60 percent meet audit requirements. In all other cases, the auditor signs the security certificate, accepting "human error" as a norm and a fixable issue.

According to The Artificial Intelligence Index Report 2024, published by the Institute for Human-Centered AI (HAI), Stanford University, "Technology Risks from AI are becoming a concern for businesses across the globe. A global survey on responsible AI highlights that companies' top AI-related concerns include privacy, data security, and reliability. The survey shows that organizations are beginning to take steps to mitigate these risks."

The bottom line is this: Be balanced with investments in technology, especially in automation and AI, identify the right use cases, build a reliable security strategy without adding to technology risks, and acquire the skills to use data and leverage AI.

In today's technology-saturated world, investing in "too much innovation" can be counter-productive. However, with sensible and sound thinking, this danger can be avoided.