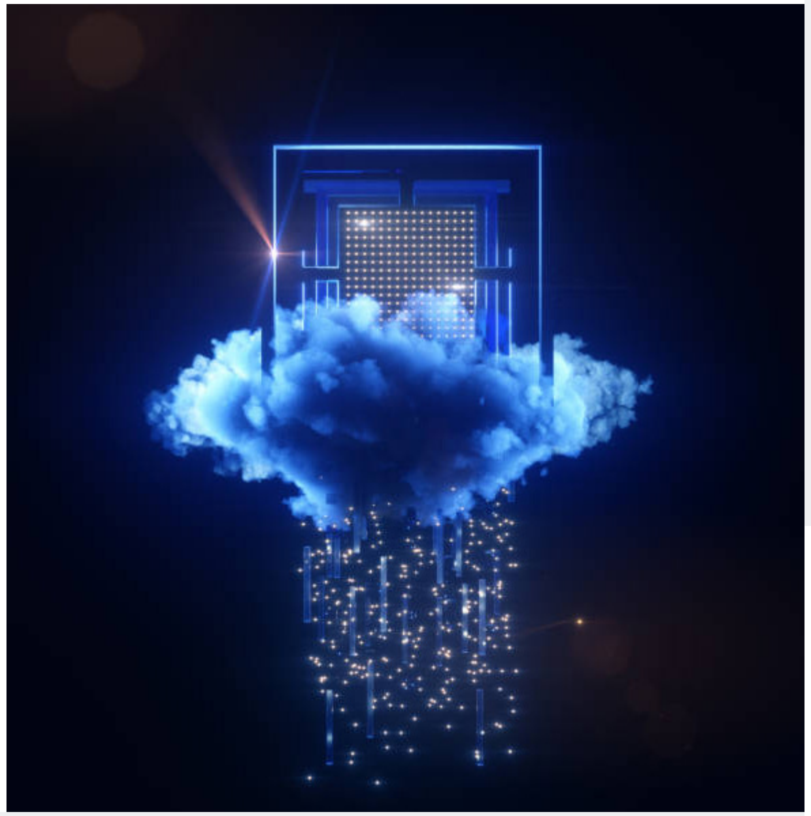
Data Privacy in the age of Digital Transformation

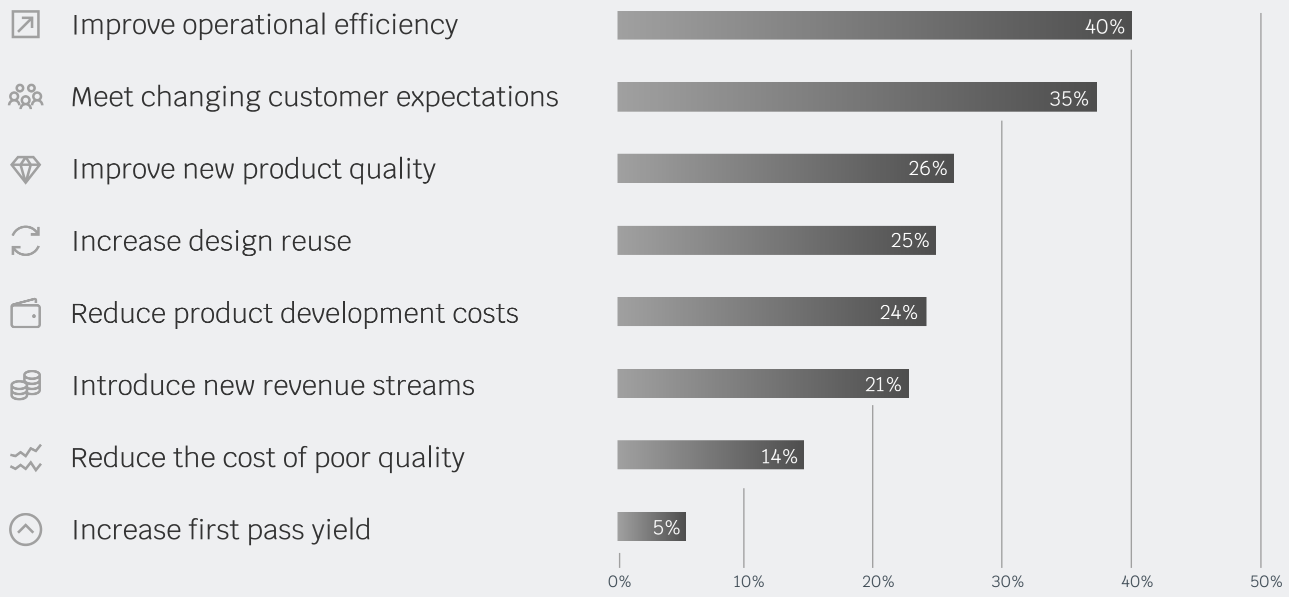
BY HAFIZ SHEIKH ADNAN AHMED

Most of us have been hearing the term "digital transformation" pretty much everywhere for a few years now. It all started by migrating business processes to automation, e-services were introduced, and with the advent and usage of mobile phones, we saw mobile apps for almost every line of business. Entire industries were transformed and moved a great deal of their activity online, embracing technologies such as cloud storage, IoT, and more. Digital transformation (DX) used to be just good to have. But since COVID-19 disrupted business operations worldwide, many organizations now see DX as a necessary step in preserving their business. The Global Digital Transformation Market is expected to grow from 469.8 Billion USD in 2020 to 1,009.8 Billion USD by 2025, at a Compound Annual Growth Rate (CAGR) of 16.5% during the forecast period.

According to Finances Online, the top benefits of adopting a digital model include improved operational efficiency, changing customer expectations, and improving new product quality.

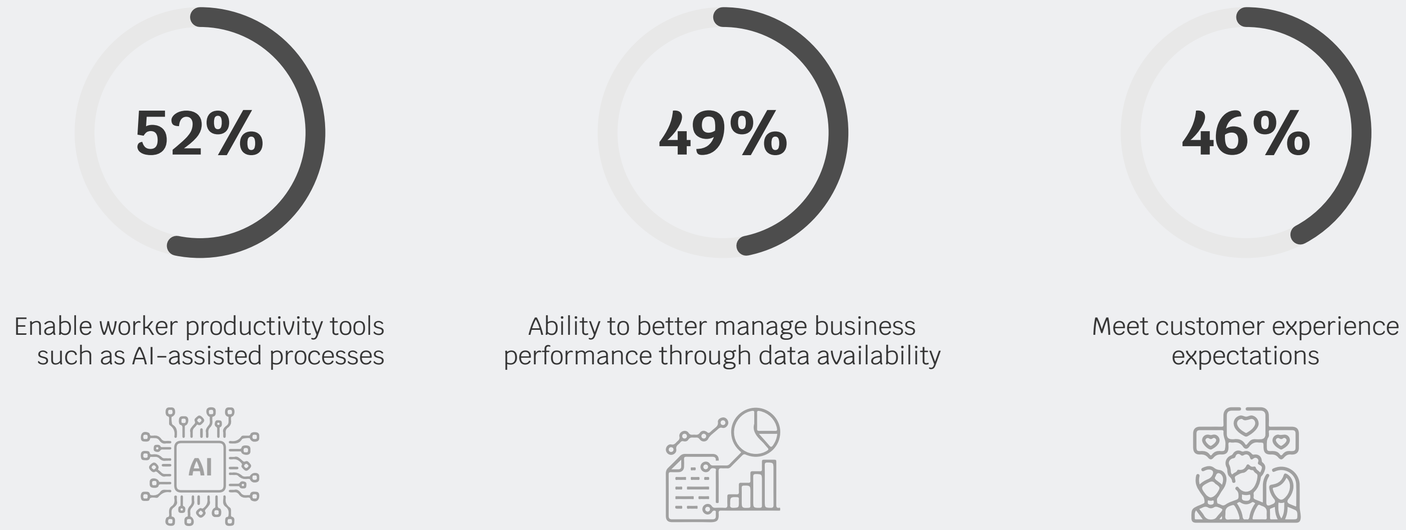


Top benefits of adopting a digital model



It is also noteworthy to understand what "digital business" does mean to organizations. It enables worker productivity through tools, such as AI-assisted processes, the ability to better manage business performance through data availability, and meet customer experience expectations.

What does "digital business" mean to organizations?



With the advent of digital transformation over the last two decades has coined a new statement "data is the new oil", and that holds true from the fact that individuals, organizations, states, and countries across the globe are realizing the importance of data and data privacy. The bad guys are as intelligent as the good guys, and they know what they are after. With the massive migration in the last couple of years to remote work due to COVID-19, making better use of the cloud has exposed more data to risk, and it is still unsure whether everybody is aware of that increased risk and how to protect it.

After the enforcement of the EU General Data Protection Regulation (GDPR) in 2018, which I consider the referring point of all modern data privacy laws and regulations, states and countries around the globe are either adopting existing data privacy laws or creating their own. According to a 2021 report, 133 jurisdictions around the world have enacted omnibus data privacy laws. Throughout the last several months, many countries have announced and enforced data privacy regulations. For example, China enacted the Personal Information Protection Law (PIPL), Saudi Arabia approved a Personal Data Protection Law that came into effect in March 2022, and the United Arab Emirates (UAE) has published the UAE Data Protection Law that introduces major changes to data protection in the UAE.

So, now we are standing at an interesting crossroads. We want things to be done in the blink of an eye, our lives are "digitalized", and are connected to devices all around. Our lives are overtaken by robotics, chatbots, virtual assistants, virtual reality, Artificial Intelligence, Machine Learning, etc. Data ownership is flawed, on paper it appears to be controlled by the one who that data belongs to, but the reality is different - data owners themselves are not aware of how their data is being shared and used. Through algorithms based on data, many organizations target ads based on your search history, in order to cater to consumers' interests and inevitably be of benefit to their business.

While digital transformation is creating major opportunities for organizations, it is also introducing a new dimension to the traditional view of risk. With industry 4.0, business leaders are making strategic choices on the investment, technology, resource levels, and skills needed to operate a digital business, all of which will have an impact on the short-term profitability and long-term viability of the organizations. These strategic choices inevitably involve an element of risk. At the same time, organizations must cope with external threats. For example, as an organization undergoes digital transformation and more of its assets become digital, the threats of cybercrime and risks around data privacy are growing.

Let us take the example of Artificial Intelligence (AI). Artificial intelligence (AI) has developed rapidly in recent years. Today, AI and its applications are a part of everyday life, from social media newsfeeds to mediating traffic flow in cities, to autonomous cars, to connected consumer devices, such as smart assistants, spam filters, voice recognition systems, and search engines.

AI has the potential to revolutionize society, however, there is a real risk that the use of new tools by states or organizations could have a negative impact on human rights. The following are some of the major data privacy risk areas and problems related to AI:

- **Reidentification and De-Anonymization** — AI applications can be used to identify and track individuals across different devices in their homes, at work, and in public spaces. For example, facial recognition, a means by which individuals can be tracked and identified, has the potential to transform expectations of anonymity in public spaces.
- **Discrimination, unfairness, inaccuracies, and bias** — AI-driven identification, profiling, and automated decision-making can lead to discriminatory or biased outcomes. People can be misclassified, misidentified, or judged negatively, and such errors or biases may disproportionately affect certain demographics.
- **Opacity and secrecy of profiling** — Some applications of AI can be obscure to individuals, regulators, or even the designers of the system themselves, making it difficult to challenge or scrutinize outcomes. While there are technical solutions to help improve some systems' interpretability or ability to audit, a key challenge remains whenever this is not possible, and the outcome can significantly impact people's lives.
- **Data exploitation** — People are often unable to fully understand what kind of — and how much — data their devices, networks, and platforms generate, process, or share. As consumers continue to introduce smart and connected devices into their homes, workplaces, public spaces, and even bodies, the need to enforce limits on data exploitation has become increasingly pressing.
- **Prediction** — AI can utilize sophisticated machine-learning algorithms to infer or predict sensitive information from non-sensitive forms of data. For instance, someone's keyboard typing patterns can be analyzed to deduce their emotional state, which includes emotions such as nervousness, confidence, sadness, or anxiety. Even more alarming, a person's political views, ethnic identity, sexual orientation, and even overall health status can also be determined based on activity logs, location data, and similar metrics.

Let us now talk about IoT or the Internet of Things. The Internet of Things (IoT) is a broad term that generally refers to physical devices connected to the internet that collect, share, or use data. This includes personal wearable devices, such as watches and glasses, home appliances such as televisions and toasters, features of buildings such as lifts and lights, supply chain and industrial machineries such as forklifts and sprinklers, and urban infrastructures such as traffic lights and rubbish bins. IoT devices and the data they collect can provide convenience, efficiency, and insights into essentially every aspect of our world. For the public sector, the IoT is currently providing many benefits and has the potential to generate even greater public value in the future.

Consumers, governments, and businesses everywhere have been increasingly using IoT devices, and it is widely expected that the use of IoT will continue to expand rapidly. However, rushing into IoT without proper consideration of privacy can lead to harmful and unexpected consequences. As IoT grows, the amount of data it generates will naturally increase alongside it. These large collections of data can, in many cases, constitute personal, health, and sensitive information, raising many privacy challenges. Some of the challenges around data protection include, for example:

- **De-Identification of IoT data** - The data collected by large IoT ecosystems like smart cities can be valuable for a range of purposes, such as research or informing policy decisions. A common way to maximize the value of this data is to make it publicly available online. However, it is generally impermissible for datasets that include personal information to be publicly available. The simplest way to ensure personal information is not included in a dataset is to allow individuals to remain anonymous by never collecting information that can identify them. However, data collected by the IoT is often very difficult to de-identify due to its highly granular nature.
- **Transparency** - The passive nature of many IoT devices can make it difficult for individuals to be informed that their personal information is being collected. Devices in public spaces can collect information automatically, sometimes relying on individuals to opt-out if they do not want their information collected.
- **Accountability** - The number of organizations that can be involved in an IoT ecosystem can make it difficult to identify who is, or should be, accountable for what. The nature of IoT devices can make it impossible for an organization to have control over every aspect of it. For example, organizations often have little or no control over security and privacy risks with communication technologies, such as satellite or 5G, as these are usually provided by third-party telecommunication companies. This can also be the case for cloud services, which can allow users to have anywhere from no control to high control over the security and privacy settings of the services they are using.
- **Interoperability** - The rapid expansion of IoT in recent years has led to the development of many kinds of devices, Application Programming Interfaces (APIs) infrastructure, data formats, standards, and frameworks. This has caused significant interoperability issues, in that devices, software, and data from one vendor often do not work with devices, software, and data from other vendors.

Data Privacy Solutions for Digital Transformation

Privacy laws have never been as important as they are today, now that data travels the world through borderless networks. Exciting times are ahead for privacy legislation as several notable privacy laws will be enforced. Cross-border transfers are likely to be one of the notable compliance issues tackled by legislative bodies and data protection authorities to ensure the regularization and normalization of data transfers between countries.

Governments around the world are reacting to the increased demand for data protection through different legislations. There is a proliferation of data protection laws during the last few years, which introduced new compliance requirements for organizations. In case of new regulations, it is vital to achieve balance between protection and free movement of sensitive data. Global compliance involves safeguarding sensitive data like payment and personal information.

The EU General Data Protection Regulation (GDPR) is a landmark privacy law and a milestone for the digital age. It has introduced new rights for individuals, such as the Right to be Forgotten and the Right to Portability, as well as made breach notification mandatory.

Something organizations should take into consideration is hiring Privacy Architects and protection officers to assess their objectives and the privacy legislation that they will have to comply with. Organizations need to ensure that DPOs (Data Protection Officers) should be experts, in both privacy and technology, a rare yet essential combination of expertise. This is not just a matter of data privacy but compliance as well.

While investing in the right security solutions will enhance the business' posture against new technology-related risks, organizations need assistance in tackling this challenge from a compliance point of view.

Organizations need to work towards implementing transparent and secure mechanisms. With the right security solutions, companies can achieve the freedom and flexibility they need to succeed in a digital economy with confidence. Organizations need to define data governance strategy and privacy/protection should be at the heart of this strategy. It should include regular training, awareness, and workshops on digital technologies and how to protect personal data while using those digital technologies. Besides external threats like phishing attacks, organizations should keep in mind to guard their sensitive data against insider threats as well. The latter requires a focus on understanding and securing the data itself. Organizations also need to employ data security governance principles by focusing on sensitive data protection and privacy, conducting, deleting unnecessary data, and consolidating data silos, whether they are on-premise or in the cloud, to ensure project alignment with business objectives.

The Final Verdict

Despite its potential pitfalls, digital transformation remains an extremely exciting venture for businesses of all shapes and sizes. The prospect of leveraging cutting-edge technology to accelerate their business processes, and thereby, making themselves more competitive is certainly attractive. However, data privacy should always be the foundation of any digital transformation project, as without it, the whole house will start to fall.

At the end of the day, companies that incorporate transparent privacy policies into the building blocks of their companies are the ones that will see increased brand loyalty moving forward. They are the ones who are actively pursuing ways to incorporate blockchain into processes and who are actively working to not just meet but exceed the guidelines of the General Data Protection Regulation. They are the ones who actively empower their customers to offer them information, knowing it will be used to enhance their user experience — no more, no less.

But in the next three to five years, I anticipate privacy will become a game-changer for the organizations that do it right. It will bolster trust and ultimately sales. And customers will, thankfully, be all the wiser for it.

Hafiz Sheikh Adnan Ahmed
IT Governance, Risk, and Compliance, Business Continuity, Information and Cybersecurity, and Data Protection Expert, Certified PECB Trainer

Hafiz Sheikh Adnan Ahmed's journey started back in 2005 as a Quality Assurance Engineer and over the years he shaped his career in the areas of Information and Communication Technology (ICT) governance, Information and Cybersecurity, Business Continuity and Organizational Resilience, Data Privacy and protection, Risk Management, enterprise excellence and innovation, and digital and strategic transformation. He is an analytical thinker, writer, certified trainer, global mentor, and advisor with proven leadership and organizational skills in empowering high-performing technology teams. He is a certified Data Protection Officer and has won Chief Information Security Officer (CISO) of the Year award in 2021 and 2022, by GCC Security Symposium Middle East and Cyber Sentinels Middle East, respectively.

Hafiz is a public speaker and conducts regular training, workshops, and webinars on the latest trends and technologies in the fields of digital transformation, information and cybersecurity, and data privacy. He is an ISO Lead Auditor and ISO Management Systems Auditor for ISO 9001, ISO 20000, ISO/IEC 22301, ISO/IEC 27001, and ISO/IEC 27701 Management Systems. He volunteers at the global level of ISACA® in different working groups and forums. He is the Co-Founder and CIO of Azaan Cybertech Consulting, and his role is to drive and align business strategies of the company's esteemed clients towards information and cybersecurity centric and to oversee the people, processes, and technologies within the organizations to ensure they deliver outcomes that support the goals of the business. To know more about Azaan Cybertech Consulting, log on to: https://azaan.net.au

Hafiz can be contacted through email at: hafiz.ahmed@azaanbiservices.com

organizations with technology transformation, cloud strategies, technology implementation, cloud security, cybersecurity resilience, and IT Disaster Recovery (DR).