

Impact Of Technology Advancement On Information Technology And Systems Industry

Posted on October 11, 2022

Introduction

Technological advancement is reshaping the information technology and systems industry by changing not only the products firms sell but also the infrastructure, skills, risks, and market power on which digital services depend. [Cloud computing](#) converted computing capacity, storage, databases, and specialized tools into services that can be rented on demand. Artificial intelligence has expanded software from explicit instructions toward systems that generate, classify, predict, and recommend. Edge computing, advanced semiconductors, mobile networks, open-source software, and data platforms connect sectors that were once managed separately. These capabilities lower some barriers to experimentation because a small organization can access powerful infrastructure without building its own data center. They can also create new dependencies on a limited number of cloud, chip, platform, and data providers. The industry's development should therefore be evaluated through both innovation and governance. Faster systems and new features matter, but long-term progress also depends on cybersecurity, interoperability, privacy, workforce capability, environmental responsibility, and the resilience of the physical infrastructure supporting apparently "digital" services.

Cloud, AI, and the Restructuring of Software

Cloud platforms changed the economics of software development by allowing firms to scale applications, databases, analytics, and machine-learning workloads without purchasing every component in advance. The same convenience can create lock-in when applications depend heavily on proprietary interfaces, data formats, or managed services that are difficult to replace. Artificial intelligence adds a second structural change. Generative and predictive systems can assist software development, customer service, search, security analysis, and decision support, but they introduce risks such as inaccurate output, biased performance, data leakage, intellectual-property disputes, and overreliance on automation. The [AI Risk Management Framework](#) emphasizes governance, context, measurement, and management rather than judging an AI system only by a successful demonstration (National Institute of Standards and Technology [NIST], 2026). Organizations therefore need documented use cases, testing, human oversight, incident processes, and clear accountability. The competitive advantage of AI increasingly depends on reliable integration and responsible operation,

not simply access to a model that competitors can also obtain.

Cybersecurity, Edge Systems, and Physical Infrastructure

As digital systems become more distributed, cybersecurity has shifted from a technical afterthought to an organizational governance responsibility. NIST's [Cybersecurity Framework 2.0](#) explicitly strengthens governance and is designed for organizations of different sizes and sectors (NIST, 2024). Cloud identities, mobile devices, application programming interfaces, software supply chains, industrial systems, and AI services all expand the attack surface. Edge computing adds devices operating near factories, vehicles, hospitals, or sensors where low latency, resilience, or privacy may justify local processing, but those devices can be physically exposed and difficult to patch. Strong systems therefore depend on inventory, multifactor authentication, least privilege, secure configuration, signed updates, backups, monitoring, and tested incident response. The hardware layer also matters. Advanced computing relies on semiconductor design tools, fabrication facilities, packaging, energy, water, and global logistics. Digital services may appear weightless to users, yet shortages, geopolitical disruption, or data-center failures can affect industries far beyond information technology because finance, manufacturing, healthcare, education, and government increasingly share the same infrastructure.

Competition, User Experience, and Workforce Change

Technological advancement lowers entry costs in some layers while increasing concentration in others. Open-source libraries and rented cloud infrastructure let small firms build products quickly, but network effects, platform rules, app-store control, access to data, and specialized hardware can strengthen incumbent providers. Competition therefore has to be examined at the layer where dependence occurs rather than by simply counting the number of applications in a market. Interoperability, data portability, transparent platform policies, and realistic exit options can give customers more control. User experience is equally important because a technically powerful system fails when people cannot understand it, recover from errors, or use it with assistive technology. Accessibility should be built into requirements rather than added after complaints. Workforce transformation follows the same pattern. Automation may reduce repetitive administration while increasing demand for cybersecurity, data governance, integration, accessibility, product management, and domain expertise. Effective digital organizations need people who can connect technology with fields such as health, law, education, finance, or manufacturing and who can evaluate automated output rather than merely produce it.

Privacy, Data Governance, and Responsible Automation

Data is often described as the fuel of the digital economy, but personal data represents people, relationships, behavior, and sometimes highly sensitive aspects of life. Collecting more information does not automatically create more value. Organizations need a defined purpose for collection, access controls, retention limits, vendor oversight, and meaningful transparency about how information is used. AI increases pressure to reuse large datasets for training or analytics, which raises questions about consent, legal authority, reidentification, model leakage, and the treatment of sensitive information. Automation also changes the consequences of error because a flawed manual decision may affect one case while a flawed automated rule can influence thousands before anyone notices. Version control, peer review, staged deployment, observability, rollback, and human escalation therefore remain important even as development becomes faster. Technology should support accountable decisions rather than obscure responsibility behind a model or workflow. The mature information-systems industry increasingly competes on trust, reliability, and governance as well as on processing speed or feature count.

Energy, Electronic Waste, and the Material Cost of Digital Growth

The environmental impact of information technology extends from data-center electricity and water use to mining, manufacturing, transport, and discarded devices. The [The Global E-waste Monitor 2024](#) reports that electronic waste is increasing faster than documented formal collection and recycling, with global e-waste projected to reach about 82 billion kilograms by 2030 under current trends (International Telecommunication Union & UNITAR, 2024). This makes [electronic waste](#) a product-design and software-support issue as well as a disposal problem. Devices can become waste prematurely when batteries cannot be replaced, parts are unavailable, or security updates end while the hardware still functions. Circular approaches emphasize durability, repair, secure reuse, component recovery, and verified recycling. Data centers also require measurement of workload efficiency, hardware utilization, cooling, electricity source, and water demand. Claims that digital services are environmentally light should therefore be evaluated across the entire lifecycle rather than only at the moment a user accesses software through a screen.

Conclusion

Technological advancement is expanding the information technology and systems industry while making its dependencies more visible. Cloud computing, artificial intelligence, edge processing, automation, and advanced hardware allow organizations to build and scale capabilities rapidly, yet

they also increase concentration, cybersecurity exposure, privacy obligations, environmental cost, and the importance of resilient supply chains. Current NIST frameworks reflect this shift by treating AI and cybersecurity as governance problems that require defined responsibility, measurement, and continuous management rather than one-time technical fixes (NIST, 2024; NIST, 2026). The industry's future should therefore be judged by more than faster processors or increasingly automated products. Progress also requires accessible design, workforce development, interoperability, reliable exit options, repairable hardware, responsible data practices, and infrastructure that can withstand failures or attack. Firms that understand technology as a social and technical system are better positioned to innovate sustainably because they can evaluate who depends on each tool, what new risks accompany adoption, and how value can be created without shifting avoidable costs onto users, workers, or the environment.

References

- International Telecommunication Union & UNITAR. (2024). *The Global E-waste Monitor 2024*.
National Institute of Standards and Technology. (2024). *Cybersecurity Framework 2.0*.
National Institute of Standards and Technology. (2026). *AI Risk Management Framework resources and updates*.