Mitigating Emerging Technology Risk

In IT, there has been a steady evolution of the same three elements: interaction, information and computation. It stands to reason that the future of IT will be determined by the march of progress along these three tracks toward three specific, convergent endgames: simplicity, intelligence and abundance. The job of leaders is not to hubristically future-proof technologies, because it is impossible.[1] The pioneering advances of today might one day be dismissed as the old way. Instead, leaders must navigate new technologies while mitigating the risk to their organizations.

Emerging Risk

The pace of technological change is constantly accelerating, driven by advances in areas such as artificial intelligence (AI), the Internet of Things (IoT) and quantum computing. IT advancements are expected to lead to new products, services and ways of working that will continually reshape the enterprise landscape. New technologies are also emerging in response to societal challenges such as climate change and demographic shifts, which will drive technological innovation and change. Organizations need to stay informed of these changes and adapt to remain competitive in the marketplace.

Although technology trends can lead to positive changes, there are also negative effects. The speed of technological change can present emerging risk. As new technologies are developed and adopted at a rapid pace, new technology risk areas emerge, and it can be difficult to keep pace and fully understand the risk and potential impacts.

Technology risk refers to the potential negative consequences that may arise from the use or misuse of technology. Some examples of technology risk include data breaches, cyberattacks, system failures and unauthorized access to sensitive information. These risk areas can have significant impacts on individuals, organizations and society. Organizations can manage technology risk by implementing security measures, developing incident response plans, and educating employees about best practices for using technology safely and responsibly.

Key IT Trends

Understanding key IT trends is essential for enterprise leaders and technologists so they can then assess the potential impact of these trends on specific strategies such as growing revenue, accelerating digital growth, maximizing value from data, and protecting and building the brand. These trends can represent a risk or opportunity for the organization and can be used to create a technology road map to drive impact on a range of strategic ambitions.

Digital Immune System

A digital immune system (DIS) is a cybersecurity concept that aims to protect digital systems and networks in the same way that the human immune system protects the body from disease. A DIS functions by monitoring the digital environment for signs of attack or infection and then deploying countermeasures to prevent or mitigate the damage. It is not a single product or solution, but a holistic approach that encompasses people, processes, and technology to protect an organization's digital assets.

TARNVEER SINGH | CISA, CRISC, CISM, CDPSE, CEH, CITP

Is security director at Cyber Wisdom Ltd. He has provided consultancy and security leadership at many large Financial Times Stock Exchange-listed businesses. He has authored several books on information security.

A DIS typically includes a combination of hardware and software solutions such as firewalls, intrusion detection systems (IDSs), and security information and event management (SIEM) tools. These systems work together to provide real-time threat detection, incident response and automated remediation capabilities.

One of the key benefits of a DIS is its ability to adapt and evolve over time to keep pace with the ever-changing threat landscape. As new threats and vulnerabilities are discovered, the DIS can be updated to incorporate new countermeasures and defenses. DIS can be used with AI, machine learning and big data technologies to create proactive, adaptive and self-healing cyberdefense mechanisms.

Applied Observability

Applied observability is the practice of using observability techniques to understand and optimize the performance and behavior of complex systems in a production environment. Observability is a set of techniques used to understand the internal state of a system without having access to its internal logic. Instead, the system behavior is observed through its inputs and outputs and by collecting and analyzing data from different sources, such as log files, traces and metrics.

Applied observability is not just a collection of tools but a culture and mindset. It emphasizes the visibility of the system to achieve understanding and make data-driven decisions.

AI Trust, Risk and Security Management

AI trust, risk and security management (AI TRiSM) is a framework used to manage risk and ensure the security of AI systems.[2] AI TRiSM aims to provide a structured approach to identifying, assessing and mitigating the risk associated with AI systems and to ensure that these systems are trustworthy and secure.

Industry Cloud Platforms

Industry cloud platforms are designed for specific industries or enterprise sectors. They provide a range of services—such as software, infrastructure and data management—that are tailored to the specific needs of the industry.

For example, a healthcare industry cloud platform can provide services such as electronic medical records (EMR) management, telemedicine and population health management. A finance industry cloud platform can provide services such as accounting, banking and securities trading.

Platform Engineering

Platform engineering involves designing, building and maintaining the underlying infrastructure and technologies that support the development and deployment of software applications. Platform engineering is concerned with the hardware, operating systems, databases, networks and other components that make up the platform. It also addresses security and compliance aspects such as ensuring that the platform is configured securely and that it meets compliance requirements.

Wireless Value Realization

Wireless value realization is the process of identifying, capturing and realizing the value of wireless technologies in an organization. This can include identifying new use cases and applications for wireless technologies, optimizing existing wireless deployments, and developing new wireless products and services.

Wireless technologies such as 5G, IoT and edge computing are creating new opportunities for organizations to improve efficiency, reduce costs and create new revenue streams. The successful realization of wireless value requires a clear understanding of business needs and objectives. Further, it requires a structured approach to identifying and capturing the value of these technologies.

Superapps

Superapps are mobile applications that combine a wide range of features and services, typically from multiple categories, into a single, unified platform—for example, WeChat, Go-Jek and Grab in Asia.[3] They are designed to meet most individuals' daily needs, from ordering food to booking a ride, communicating with friends, paying bills and shopping online. They are also called superplatforms or all-in-one apps.

A superapp typically enables users to access a variety of services and features such as messaging, social media, ecommerce, payments and transportation all within the same app. Superapps leverage the power of mobile technology to provide users with seamless, convenient and personalized experiences.

However, superapps also present risk. Challenges include regulatory issues, data privacy and security, and the potential for market concentration.

Adaptive AI

Adaptive AI refers to AI systems that can adapt and improve over time based on new data, experiences and feedback. These systems are also referred to as learning AI or self-adaptive AI.

LOOKING FOR MORE?

- Read *Rethinking Data Governance and Data Management. www.isaca.org/rethinking-data-governance*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Adaptive AI systems use machine learning algorithms to continuously improve their performance and decision-making processes. They learn from new data, adjust their parameters and improve their predictions or actions over time.

The goal of adaptive AI is to create systems that can operate in dynamic and uncertain environments and can improve their performance and decision-making as they gain more experience and knowledge. However, adaptive AI systems also present several challenges such as data bias, interpretability and safety.

Metaverse

The "metaverse" is a term used to describe a virtual world or universe that is created by the convergence of virtual reality, augmented reality and the Internet. It is a shared, persistent and immersive digital space where people can interact, communicate and transact with each other and with digital entities and objects.

The concept of the metaverse has been popularized in science fiction and video games, but it is rapidly becoming a reality as advances in technology such as virtual and augmented reality, 5G networks and edge computing are making it possible to create more immersive and interactive digital experiences.

The metaverse has the potential to revolutionize many aspects of society, such as entertainment, education and commerce. It can enable new forms of social interaction, such as virtual parties, concerts and gatherings. It can also create new opportunities for remote work, learning and training. The metaverse is still in an early stage of development, and it will be important to establish standards and protocols to ensure interoperability and compatibility between different platforms and ecosystems.

Sustainable Technology

Sustainable technology refers to the use of technology to promote environmental and social sustainability. It involves the design, development and implementation of technologies that are environmentally friendly, socially responsible and economically viable. Examples of sustainable technology include:

- Renewable energy technologies that produce clean and renewable energy, such as solar, wind and hydropower
- Energy efficiency technologies that reduce energy consumption, such as LED lights, smart appliances and automated building systems

> The goal of adaptive AI is to create systems that can operate in dynamic and uncertain environments and can improve their performance and decision-making as they gain more experience and knowledge.

- Sustainable transportation technologies that reduce emissions and improve air quality, such as electric vehicles and public transportation systems
- Sustainable agriculture technologies that use less water and pesticides and can be grown in urban areas, such as precision farming and vertical farming
- Recycling and waste management technologies that reduce waste and pollution, such as composting, bio-gas generation and 3D printing

Sustainable technology can help organizations and individuals reduce their environmental footprint, lower their energy costs and improve their social impact. It can also create new business opportunities and jobs in the growing sustainable technology sector.

The 2030 Agenda for Sustainable Development, adopted by all members of the United Nations in 2015, provides a shared blueprint for peace and prosperity for people and the planet, now and into the future. At its heart are 17 sustainable development goals (SDGs), which are an urgent call for action by all countries in the global partnership. Adoption of sustainable technology is critical for achieving these SDGs and addressing global challenges such as climate change, environmental degradation and social inequality.[4]

Managing Emerging Technology Risk

Organizations can manage the risk associated with changing technology by implementing a variety of strategies and best practices, such as:

- **Understanding the business strategy**—Determining the business drivers and key problems that the organization faces is a crucial first step. Emerging technological innovation can then be studied to match the problem with the right technology solutions. It is important that IT understand the wider strategy, drivers and problems.

> To mitigate the risk associated with the speed of technological change, organizations can invest in technology foresight and monitoring efforts to stay informed about emerging technologies and their potential risk.

- **Developing a technology strategy**—Having a clear understanding of the technologies that are being used and how they will be used in the future. This includes identifying key technologies that are critical to the organization's operations and developing a strategy for how they will be implemented and managed.
- **Conducting regular risk assessments**—Conducting regular assessments of the risk associated with technology deployments and developing plans to mitigate or manage the risk. This includes identifying potential vulnerabilities and attack vectors and implementing security controls to protect against them.
- **Implementing incident response plans**—Putting robust incident response plans in place to respond to security breaches and other technology-related incidents quickly and effectively. These plans should include procedures for identifying and containing security incidents and for restoring normal operations.
- **Keeping up to date with technology trends**—Staying informed about the latest technology trends and developments and how they may impact the organization. This includes monitoring the latest threats and vulnerabilities and keeping informed of new technologies that may provide opportunities for the organization.
- **Investing in training and education**—Investing in training and education to ensure that everyone is aware of best practices for using technology safely and responsibly. This includes providing training on security awareness and the use of specific technologies.
- **Building partnerships and collaborations**—Building partnerships and collaborations with other organizations and technology providers. This can aid knowledge sharing and best practices and provide access to new technologies and solutions.

Conclusion

The speed of technological change can present several risk factors to an organization. As new technologies are developed and adopted at a rapid pace, it can be difficult to keep pace and fully understand the risk and potential impacts. This can lead to a lack of readiness to deal with the consequences of new technologies, such as data privacy issues or cybersecurity threats.

In addition, the rapid pace of technological change can lead to job displacement as certain roles and industries become automated or obsolete. It can outpace regulations and laws, creating a legal and ethical grey area. For example, emerging technologies such as AI and biotechnology are raising new ethical questions that existing regulations may not address.

To mitigate the risk associated with the speed of technological change, organizations can invest in technology foresight and monitoring efforts to stay informed about emerging technologies and their potential risk. They can also engage in proactive risk management to address potential issues before they arise and be ready to adapt their policies and processes as needed.

Endnotes

[1] Bechtel, M.; "Tech Trends 2023 Prologue," Deloitte, 6 December 2022, *https://www2.deloitte.com/us/en/insights/focus/tech-trends.html#read-the-prologue*

[2] FAIRLY, "AI TRiSM: AI Trust, Risk and Security Management," *https://www.fairly.ai/blog/ai-trism-ai-trust-risk-security-management*

[3] Ajene, E.; "The Gojeck and Grab Super App Playbook," *Medium*, 10 September 2020, *https://medium.com/@eajene/the-gojek-grab-super-app-playbook-96c3db1c430a*

[4] United Nations Department of Economic and Social Affairs, "The 17 Goals," *https://sdgs.un.org/goals*