Human Error

A Vastly Underestimated Risk in Digital Transformation Technology

Também disponível em português
www.isaca.org/currentissue

There should be no doubt that digital transformation is an organizational necessity performed in the interest of maintaining, sustaining and enhancing an enterprise's relevance to its constituents. Specifically, relevance can concern everything from attracting customers in the private sector to increasing the convenience of and access to government services by citizens.

While there has been a strong focus on the "digital" aspect of digital transformation, the conversation has increasingly taken a more inclusive view of the impact of digital transformation on an enterprise—its customers, operating model and business model.[1]

Awareness of the extensive human risk factors extant in digital transformation needs to be enhanced.

Overview of Digital Transformation Technologies

Of all the emerging technologies out there, a number of them have been identified as being most likely to change the way organizations do business.[2] Given the dynamic nature of technological development, this list is subject to change, but there are several technologies that are most relevant today.

Drones

Drones, or unmanned aerial vehicles (UAVs), were originally built for military purposes.[3] They represent a convergence of several technologies, including robotics, artificial intelligence (AI) and aeronautics.

In 2013, one reason for the high number of drone crashes was believed to be the variety of control interfaces used for piloting the vehicles, resulting in the creation of the American National Standards Institute/Human Factors and Ergonomics Society (ANSI/HFES) 100-2007, with the goal of standardizing the control interface.[4] However, by 2016, technology was cited as the major cause of drone crashes, specifically, the loss of signal between the operator and the drone.[5] In a military context, drones are subject to human error and can have a negative impact on civilian life.[6]

Robotics

Robotics is also a convergence of technologies, including mechanical engineering, electronic engineering and computer science.

The word "robot" is "derived from the Czech word *robota*, meaning serf or laborer."[7] Robots need robust programming to be fully productive, and at this point, humans are still tasked with their programming. In spite of the right skills and due diligence, human coding errors can and do occur, disrupting workflow and production while codes are

Guy Pearce, CGEIT
Is the chief digital transformation officer at Convergence. He has also served on governance boards in the fields of banking and financial services, for a not-for-profit, and as chief information security officer of a financial services organization. Pearce has more than a decade of experience in data governance and IT governance and created a Digital Transformation course for the University of Toronto SCS (Ontario, Canada). He is the recipient of the 2019 ISACA® Michael Cangemi Best Author Award for contributions to the field of IT governance.

"AI IS PROGRAMMED BY HUMANS AND, THAT AGAIN, IS EXACTLY WHERE THE ISSUES CREEP IN TO CREATE RISK."

debugged, which can cost enterprises significant time and money.[8] Improper or erroneous maintenance can result in a malfunctioning robot, which can also be costly.[9]

Blockchain

While blockchain technology has moved beyond the hype of 2018, there are organizations that are using blockchain to solve real business problems, such as the sustainable production of cashmere in Mongolia.[10]

Although errors in blockchain are rare, the point of interface between the blockchain and other websites, interfaces and platforms is where human error can occur, and this needs to be resolved by deeper developer education.[11] Also, it is important to remember that when blockchain is used as a database, those data are subject to the same human shortcomings as any other database.[12] Integration risk and software vulnerability are the greatest human risk factors in this technology.[13]

3D Printing

With 3D printing, three-dimensional objects are formed layer by layer using a wide range of materials, rather than being created by skilled, precision artisans. This technology is used in manufacturing, where human error is a bigger factor than in other sectors.[14]

As with other emerging technologies, the lack of expertise and the software development requirements associated with 3D printing[15] still present human risk associated with the technology. While there are still challenges with the use of 3D printing in healthcare,[16] errors introduced due to human error in this sector can also have ethical consequences.

Internet of Things and Industrial Internet of Things

Faster Internet speeds with higher bandwidths have led to a proliferation of devices that can communicate with a central device or with other devices. This trend will accelerate with the adoption of 5G. Although a smartphone can be considered a type of Internet of Things (IoT) device with features such as a Global Positioning System (GPS) and a three-axis accelerometer, the Industrial Internet of Things (IIoT) explicitly involves industrial-grade, rugged, low-power (remote) sensors.

Again, the human risk factors in IoT and IIoT are related to programming and the hardware design of IoT and IIoT devices themselves.[17] Furthermore, these devices are often manufactured by robots, which have their own human challenges (as mentioned earlier), leading to a cascade of human risk factors. One of the greatest human risk factors, though, is found in cybersecurity,[18] and people are recognized as "the weakest link in information security."[19]

AI

Autonomous thinking machines have captured the human imagination for years, leading to scary stories about a world ruled by intelligent robots. However, because today's digital society is based on software that is vulnerable to programming failure and cyberattack, this singularity—the point where AI exceeds human intelligence—is highly unlikely.[20]

AI is programmed by humans and, that again, is exactly where the issues creep in to create risk. AI is deployed in drones, robots, IoT and IIoT devices. Human errors are, therefore, amplified and added to the errors occurring in the integrated technology. However, there is a more subtle risk associated with AI, which stems from the fact that AI is rife with human bias.[21] Because AI needs humans to validate its outcomes,[22] at least initially, human error can creep in to impact outcomes. Another issue is the quality of the data used to train AI systems. Based on experience, data quality is almost never as good as it needs to be.

Augmented Reality/Virtual Reality

In one sense, virtual reality (VR) is a digital twin of the reality it models. Augmented reality (AR), by contrast, adds to the VR experience. For example, Google Lens provides additional information about the physical reality with which one is interacting.

Again, sensors pick up information, and its interpretation is determined by programming. Likewise, the quality of the augmentation is determined by the quality of the programming. If something observed in the physical reality is not in the VR "dictionary," it might not be depicted as intended in the virtual rendition. So the quality of the AR/VR experience depends on the quality of data it receives by means of the relevant sensors and by means of the data used to create the model for the recognition engine, the latter of which may be negatively influenced by human deficiencies during modeling and programming.

Next Wave Technologies on the Doorstep

Major new technologies will continue to change the way business is conducted. Cloud technology is already here, and others such as 5G, serverless computing and biometrics must be considered. Again, each emerging technology involves human risk factors that are worth analyzing as part of a diligent digital transformation strategy.

Human Risk Factors

Based on the previous discussion, the common human risk elements in all the digital transformation technologies can be linked to programming, design and data. In other words, the same human endeavors that produce digital transformation technologies are the same ones that put them at risk.

To extend the analysis, IT risk can be considered across seven subdisciplines: cybersecurity, resilience, vendors and third parties, projects and change, software development life cycle (SDLC), data, and compliance.[23] SDLC refers to the process of producing software, whether agile or waterfall; it starts with architectural approval and concludes with deployment and maintenance. Each of these subdisciplines have human risk components:

1. **Cybersecurity**—"Countering cyber threats requires a focus on people and behaviours, not just technology."[24]
2. **Resilience**—"Human risk is neglected in disaster plans."[25]
3. **Vendors**—Performing vendor due diligence is a human-intensive effort, and errors can and do occur.

> "HUMAN ERRORS IN DATA CAPTURE, DATA TRANSFORMATION AND DATA MIGRATION HAVE BEEN AROUND FOR AS LONG AS THE COMPUTER ITSELF."

4. **Projects**—Managing change is part of a successful deployment and, for the most part, that change demands an alteration in human behavior to ensure desirable outcomes.
5. **SDLC**—Humans assess the architectural implications of a new technology, design the programs (and devices), write the programs and, to a large extent, test the programs, especially in complex deployments. Wherever humans are involved, errors are bound to be made
6. **Data**—Human errors in data capture, data transformation and data migration have been around for as long as the computer itself.
7. **Compliance**—Many compliance requirements are met by a set of rules, but some are open to interpretation. It may be human nature for the interpretation to err on the side of the organization, rather than in terms of the spirit of the legislation.

When assessing the risk related to an organization's digital transformation technology, it may be meaningful to create a table summarizing the relevant risk areas and then capture the details of each cell in a typical risk management framework (e.g., identify, analyze, evaluate, control, monitor, report). **Figure 1** illustrates the human risk elements (X) at the intersection of the seven IT risk subdisciplines and the most significant digital transformation technologies identified earlier. The dark pink shaded cells represent topics discussed in text. The interpretation of these risk domains depends on the incremental risk profiles of the specific deployments of the digital transformation technologies.

In **figure 1,** it can be noted that resilience is especially relevant to robotics and IoT/IIoT, given

Figure 1—Human Risk Elements Based on IT Risk in Digital Transformation Technologies

		Digital Transformation Technologies						
		Drones	Robotics	Blockchain	3D Printing	IoT and IIoT	AI	AR/VR
IT Risk Subdisciplines	Cybersecurity					X		
	Resilience		X		X	X		
	Vendors	X	X	X	X	X	X	X
	Projects	X	X	X	X	X	X	X
	SDLC	X	X	X	X	X	X	X
	Data	X	X	X	X	X	X	X
	Compliance	X	X					

how critical these technologies are to the manufacturing sector. There is an across-the-board impact in the vendors, projects, SDLC and data subdisciplines, especially in large organizations. In particular, the data category entails both a human input risk and an output risk—that is, the human risk related to analyzing, interpreting and acting upon the data produced by a digital transformation technology. In the compliance category, in addition to ANSI/HFES 100-2007, International Organization for Standardization (ISO) ISO 9000 *Quality management* is important for manufacturing in which robotics plays a part.

Taking Steps to Reduce Human Error

IT audits have traditionally focused on resources when considering technology risk, but from the preceding analysis, it is clear that the (human) resource implications are much more significant than previously thought. As a result, the goal should be to reduce the incidence of human error. There are three capabilities that can lead to a reduction in human error:[26]

1. **Detectability**—The ability to identify mistakes and prevent them from occurring
2. **Traceability**—The ability to identify the root cause of the mistake and institute corrective actions
3. **Dexterity**—The ability to perform a task without incurring error

Each of these capabilities can be reinforced by a culture that supports suitable training and processes. The question is whether the incremental costs required to implement these measures are considered worthwhile in the context of mitigating the potential costs of an error.

Ultimately, whatever steps are taken to reduce human error, auditors should "maintain sufficient professional skepticism when reviewing management's risk assessment for new systems"[27] by considering people as a driver (cause) of risk rather than merely reporting on its symptoms (e.g., "buggy" code).

> “IT AUDITS HAVE TRADITIONALLY FOCUSED ON RESOURCES WHEN CONSIDERING TECHNOLOGY RISK, BUT…IT IS CLEAR THAT THE (HUMAN) RESOURCE IMPLICATIONS ARE MUCH MORE SIGNIFICANT THAN PREVIOUSLY THOUGHT.”

Conclusion

Figure 1 illustrates that the human risk element is pervasive in digital transformation technology. It is present in each of the digital transformation technologies discussed in this article and in each of the subdisciplines of IT risk. The scale of human risk in digital transformation is expansive, necessitating an intense focus on people and behavior (culture) when striving to implement a successful digital transformation strategy, including mechanisms that explicitly focus on reducing the incidence of human error.

Importantly, the cascading effect of human error occurring when the human risk in one technology (e.g., AI) is introduced into another technology that has its own human risk elements (e.g., drones) means that risk management becomes more complex. Urgent measures are needed to ensure the sustainability of not only the new technology, but also of the organization deploying the new technology and to guarantee the success of the digital transformation strategy.

Given the scale of the human risk elements identified in digital transformation technology, it should be obvious that merely performing some quick “change management” intervention after deployment will be insufficient (part of the “Projects” row in **figure 1**). The human factor is present in almost every element of digital transformation, meaning that special, extended attention is needed to mitigate the associated risk and, ultimately, to ensure the success and sustainability of the digital transformation initiative.

Endnotes

1. Pearce, G.; “Enhancing the Board’s Readiness for Digital Transformation Governance,” *ISACA® Journal*, vol. 5, 2019, *https://www.isaca.org/archives*
2. Pearce, G.; “Acknowledging Humanity in the Governance of Emerging Technology and Digital Transformation,” *ISACA Journal*, vol. 4, 2019, *https://www.isaca.org/archives*
3. Vyas, K.; “A Brief History of Drones: The Remote Controlled Unmanned Aerial Vehicles (UAVs),” *Interesting Engineering*, 2 January 2018, *https://interestingengineering.com/a-brief-history-of-drones-the-remote-controlled-unmanned-aerial-vehicles-uavs*
4. Atherton, K. D.; “What Causes So Many Drone Crashes?” *Popular Science*, 4 March 2013, *https://www.popsci.com/technology/article/2013-03/human-error-after-all/*
5. *Business Insider*, “Drone Accidents Are Due to Tech, Not Human Error,” 25 August 2016, *https://www.businessinsider.com/drone-accidents-due-to-tech-not-human-error-2016-8*
6. King, T.; “Positive and Negative Effects of Drones,” Positive Negative Impact, 8 July 2019, *https://positivenegativeimpact.com/drones*
7. Hockstein, N. N.; C. G. Gourin; R. A. Faust; D. J. Terris; “A History of Robots: From Science Fiction to Surgical Robotics,” *Journal of Robotic Surgery*, 17 March 2007, *https://link.springer.com/article/10.1007/s11701-007-0021-2*
8. Matthews, K.; “Four Reasons You Still Need to Watch for Human Error When Working With Robotics,” RobotIQ, 22 November 2018, *https://blog.robotiq.com/4-reasons-you-still-need-to-watch-for-human-error-when-working-with-robotics*
9. *Ibid*.
10. Huang, R.; “UN Pilot in Mongolia Uses Blockchain to Help Farmers Deliver Sustainable Cashmere,” *Forbes*, 28 December 2019, *https://www.forbes.com/sites/rogerhuang/2019/12/28/un-pilot-in-mongolia-uses-blockchain-to-help-farmers-deliver-sustainable-cashmere/#60cedd8717d9*
11. Tanase, B.; “Human Error as a Limitation for Blockchain Adoption?” *Medium*, 21 December 2017, *https://medium.com/@biancatanase/human-error-as-a-limitation-for-blockchain-adoption-80f3da30e8be*

Enjoying this article?

- Read *The Future of IT Audit. www.isaca.org/Future-of-IT-Audit*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

12 Davies, C.; "Blockchain's Issues and Limitations," Cryptoboom, 9 December 2017, *https://cryptoboom.com/basics/blockchain/blockchains-issues-and-limitations*

13 Raman, R.; M. Mangnaik; "Blockchain Can Transform the World, but Is It Fool-Proof?" *Huffington Post*, 24 January 2017, *https://www.huffingtonpost.in/raja-raman/blockchain-can-transform-the-world-but-is-it-fool-proof_a_21660586/*

14 Wright, I.; "Human Error Is Worse in Manufacturing Compared to Other Sectors," *Engineering.com*, 8 November 2017, *https://www.engineering.com/AdvancedManufacturing/ArticleID/15974/Human-Error-is-Worse-in-Manufacturing-Compared-to-Other-Sectors.aspx*

15 Tractus3D, "3D Printing for Manufacturing," *https://tractus3d.com/industries/3d-printing-for-manufacturing/*

16 Wright, C.; "3D Printing in Healthcare," PreScouter, April 2017, *https://www.prescouter.com/2017/04/3d-printing-healthcare/*

17 Joyce, J.; "How the Internet of Things Is Affecting Laboratory Equipment," *Lab Manager*, 7 May 2018, *https://www.labmanager.com/laboratory-technology/2018/05/how-the-internet-of-things-is-affecting-laboratory-equipment*

18 *Ibid*.

19 Lineberry, S.; "The Human Element: The Weakest Link in Information Security," *Journal of Accountancy*, 1 November 2007, *https://www.journalofaccountancy.com/issues/2007/nov/thehumanelementtheweakestlinkininformationsecurity.html*

20 Thomas, M.; "Human Error, Not Artificial Intelligence, Poses the Greatest Threat," *The Guardian*, 3 April 2019, *https://www.theguardian.com/technology/2019/apr/03/human-error-not-artificial-intelligence-poses-the-greatest-threat*

21 *Op cit* Pearce, "Acknowledging Humanity in the Governance of Emerging Technology and Digital Transformation"

22 Kent, J.; "Artificial Intelligence Success Requires Human Validation, Good Data," *Health IT Analytics*, 26 November 2019, *https://healthitanalytics.com/news/artificial-intelligence-success-requires-human-validation-good-data*

23 McKinsey & Company, "'The Ghost in the Machine': Managing Technology Risk," July 2016, *https://www.mckinsey.com/business-functions/risk/our-insights/the-ghost-in-the-machine-managing-technology-risk*

24 Walker, E.; D. Witkowski; S. Benczik; P. Jarrin; "Cybersecurity—The Human Factor," Federal Information Systems Security Educator's Association, 2017, *https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017_Witkowski_Benczik_Jarrin_Walker_Materials_Final.pdf*

25 Ashford, W.; "Human Risk Is Neglected in Disaster Plans, Warns Study," *Computer Weekly*, 9 November 2007, *https://www.computerweekly.com/news/2240083858/Human-risk-is-neglected-in-disaster-plans-warns-study*

26 Nakata, T.; "Human Error Prevention," Slideshare, 19 December 2011, *https://www.slideshare.net/torunakata/human-error-prevention*

27 Lindsay, J. B.; A. Doutt; C. Ide; "Emerging Technologies, Risk, and the Auditor's Focus," Harvard Law School Forum on Corporate Governance, 8 July 2019, *https://corpgov.law.harvard.edu/2019/07/08/emerging-technologies-risk-and-the-auditors-focus/*