Technology

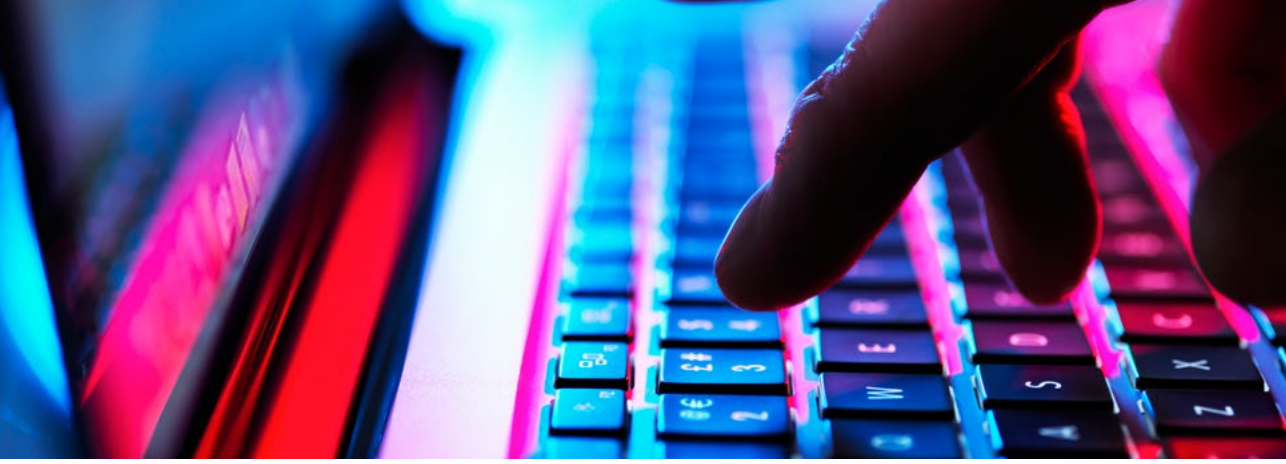
wtwco.com

Technology

2022 proved to be no exception to the accelerated adoption of technology that began alongside the onset of the COVID-19 pandemic. From the development of artificial intelligence (AI) and machine learning (ML) to the expansion of digital worlds via the Metaverse, technology advances show no signs of abating.

Adjusting to the new realities of the pandemic, companies have had to adapt their workforces, business models, and organizational cultures to fit in an increasingly connected and technological world. Many of these advancements will challenge society's basic assumptions but companies must be willing and able to take the initiative on crucial investments in both platforms and individuals going forward.

As nearly every organization will develop and incorporate digital technologies within their business structure, having a solid foundation built around adaptive principles and a nimble workforce will be crucial for companies to have a leading edge.



The past year gave way to a whole new paradigm surrounding issues such as natural language processing (NLP), cyber security, large language models (LLM), the metaverse, quantum computing, and individual rights in the digital space.

Much of our current modes of operations and organizational architectures are based on the Internet as we know it today. However, many of the most recent technological progressions such as the Metaverse and Web3 don't abide by the traditional constraints that have defined the Internet over the last three decades. Building the next generation of services will depend greatly upon the mastery of new domains, especially over the medium term.

Technological disruptions will become more norm than aberration as new paradigms will continue to emerge in the innovation landscape.

The widespread adoption and use of ChatGPT presents a particular salient example. As the most well-known of the LLMs currently in use, it has proliferated at an exponential rate, spurring rival companies to quickly bring their products to market in order to compete in the predictive text realm. Cybersecurity also represents a significant disruptor as cyber-attacks have been on the uptick compared to recent years with both governmental and non-governmental infrastructure targeted. Individuals will also experience significant digital disruption in a personal and professional capacity as remote works begins to take shape in a post-pandemic world.

The WTW Research Network has worked closely with multiple universities and organizations to better understand these developments. Partnering with Warwick University, we looked at how AI can be utilized for cybersecurity and the ways AI techniques can help corporates make their structures more resilient to cyber attacks. We also looked at the importance of cyber bullying insurance in mitigating online crimes and how companies' human resources practices can be amended to implement protections for minors as part of a larger benefits packages for their employees. And our work with Wharton's Mack Institute continues, examining issues such as the future of digital skills, disruptive technologies, and key megatrends that will shape the technology landscape in the coming years.

Omar Samhan
People and Technology Risk Analyst

Personal Identity Insurance: Coverage and Pricing in the US

Personal identity theft occurs when a criminal uses stolen personal identifiers to manipulate third-parties into taking actions under the false belief they are communicating with the individual whose identity has been stolen

A typical example is the criminal taking a loan out under someone else's name or tricking tax authorities into sending the rebate to the criminal's account. A market for personal identity insurance has emerged to mitigate the associated harms.

In work conducted by Daniel Woods at the University of Edinburgh as part of a broader WTW Research Network program looking at Trust in Technology, we investigate personal identity insurance in the context of societal and financial harms and negative externalities in the form of lost income, attorney fees, and even mental health counseling.

There is a risk of identity theft whenever third parties use personal identifiers to decide whether and who to send funds to. Historically, debt was issued by a member of the local community who could authenticate an individual via natural identifiers such as face, voice, gait, and so on[1]. Such identifiers are not readily available when banks extend credit to individuals from distant parts of the country, let alone to international borrowers.

To solve this problem, lenders authenticate distant applicants via personal identifiers—passport details, social security numbers, address and so on—that are presumed to be known by the individual alone. This assumption is flawed because of the billions of personal records that have been lost in corporate data breaches over the last three decades[2,3]. Criminals can use the stolen data to trick lenders into sending the loan payment to the criminal.

The economic costs of identity theft raise the possibility that individuals can insure against the consequences of identity theft. In this project we collected a sample of 34 policies available in the US from a regulatory database and conducted an inductive content analysis of the policy documents and pricing algorithms, which allows us to answer the following three research questions:

[1]David Graeber. Debt: The first 5000 years. Penguin UK, 2012.

[2]Benjamin Edwards, Steven Hofmeyr, and Stephanie Forrest. Hype and heavy tails: A closer look at data breaches. Journal of Cybersecurity, 2(1):3–14, 2016.

[3]Maochao Xu, Kristin M Schweitzer, Raymond M Bateman, and Shouhuai Xu. Modeling and predicting cyber hacking breaches. IEEE Transactions on Information Forensics and Security, 13(11):2856–2871, 2018.

1

Which harms are covered by personal identity insurance?

2

What is the implied likelihood and severity of each harm?

3

How do insurers justify the scope and pricing of coverage?

The study also contributes to an emerging field of technology insurance that covers cyber attacks[4], crypto assets[5], cyber bullying[6] and artificial intelligence liability[7]. So far, corporate cyber insurance is the only technology insurance product with a developed body of literature. Research into cyber insurance has also considered whether it improves social welfare and how this motivates different regulatory strategies[8, 9]. These questions typically turn on whether insurers improve risk management processes. More research is required to answer whether personal identity insurance does so, although we have argued identity theft is largely outside the individuals' control.

This study confirms one aspect of the privacy/harm literature as evidenced by the emergence of a private market covering the harms associated with identity theft incidents. We provide an additional contribution, namely that the lack of support services leads individuals to suffer more harm. For example, one insurer anticipates case management services lead to a 90% reduction in the cost of an identity theft incident. Thus, policy makers could reflect on whether the impacts of identity theft and the expertise to remedy them are fairly distributed across society. The status-quo in which financial smoothing and risk reduction services are privately provided undoubtedly skews towards affluent consumers.

[4] Sasha Romanosky, Andreas Kuehn, Lillian Ablon, and Therese Jones. Con- tent analysis of cyber insurance policies: how do carriers price cyber risk? Journal of Cybersecurity, 5(1), 2019.

[5]Adam Zuckerman. Insuring crypto: The birth of digital asset insurance. U. Ill. JL Tech. & Pol'y, page 75, 2021.

[6]Nir Kshetri and Jeffrey Voas. Thoughts on cyberbullying. Computer, 52(4):64–68, 2019.

[7]Anat Lior. Insuring AI: The role of insurance in artificial intelligence reg- ulation. Harvard Journal of Law and Technology, (1):in print, 2022.

[8]Jan Martin Lemnitzer. Why cybersecurity insurance should be regulated and compulsory. Journal of Cyber Policy, in print, 2021.

[9]Tom Baker and Anja Shortland. The government behind insurance governance: Lessons for ransomware. Regulation & Governance, 2022.

Artificial Intelligence in the role of assessing cyber risk

Since the onset of the Covid-19 pandemic, industries across the globe have witnessed a sharp rise in the number and types of cyberattacks they face.

Understandably, cyber risk management systems have been unable to keep up with these sophisticated security attacks. With businesses trying to cut down their labor costs and adopt a cheaper and more efficient digital model, it is evident that cybercrime is also on the rise.

In recent years, insurance companies have become a target of ransomware attacks as they play a crucial role in protecting high-value assets, people, and commodities. This is where artificial intelligence (AI), if employed effectively, could help combat these threats. Integrating cyber security with AI helps one develop a more holistic and robust model, efficient at performing various tasks such as detecting and preventing cyber-attacks in real-time, resisting novel cybercrime and increasing the competence of cyber security teams.

In a special report, The University of Warwick produced this systematic literature review that presents an overview of the barriers and opportunities of using artificial intelligence to help reduce cyber risk and threat exposure in the insurance sector.

Outputs include:

1	A systematic literature review of the state-of-the-art and emerging AI techniques with applications in risk and threat assessment.
2	Examine the barriers and opportunities of utilizing AI techniques for decision-making in the insurance industry.
3	Review the efficacy of emerging AI techniques in identifying unknown adversarial scenarios and feared events – and how these affect traditional risk assessment processes.
4	Provide a set of recommendations that can act as a guideline/roadmap for different stakeholders in that industry.

Systematic review of emerging AI techniques with applications in risk and threat assessment

With an increase in the use of AI throughout multiple industries, the insurance industry today stands on the edge of large-scale adoption of the technology. This work with the University of Warwick provides an approach to understanding how emerging and state-of-the-art AI technologies can be used to reduce risks and better the security posture of an organization.

The employment of AI in insurance innovation is now used for a variety of back-end functions such as fraud detection, algorithmic trading, blockchain analytics, and financial search engines. Robotics, computer vision, and Natural Language Processing (NLP) are some fields that are being serviced by machine learning (ML). These applications have increased interest in machine learning within the insurance sector, which is rich in data. Examples of ML techniques include:

- **Support Vector Machines** – an ML algorithm that learns from examples it is given. When many fraudulent and non-fraudulent activity reports are examined, it can identify credit card fraud.
- **Artificial Neural Network** – the primary focus is the use of an improved neural network for assessing information risk. The purpose of neural networks is to resemble the human brain.
- **Decision Tree** – a tool that forecasts potential outcomes, such as resource costs and utility, using a tree-like model of possibilities.
- **Naïve Bayes** – a straightforward "probabilistic classifier," the Naïve Bayes classifier is based on the Bayes theorem and robust (naive) independence assumptions.
- **Random Trees** – this learning method is made to handle issues like regression and other difficulties that need the training of many decision trees.

The main advantage of using AI in the insurance sector is that it makes data management simpler. Datasets that are semi-structured and unstructured can be organized using machine learning. Datasets from various insurance companies are available for scholars and data analysts to utilize. Machine learning may be used in the insurance industry to identify risk, claims, and consumer behavior with greater prediction accuracy.

AI could also be used in various ways in the insurance industry, from responsive underwriting and premium leakage to expenditure control, arbitration, litigation, and fraud detection.

This issue is being addressed in great detail by incorporating potent artificial intelligence methods into insurance data. Many scientists are looking at cutting-edge machine-learning techniques for responsibilities, such as premium leakage to expenditure management, debt recovery, proceedings, and fraud detection, motivated by industrial production for management solutions and the academic ability to develop highly relevant machine-learning techniques.

Opportunities and barriers: utilizing AI techniques for the insurance industry

The insurance industry is made up of several key components, including fraud detection, claim prediction, risk prediction, and underwriting.

A number of industries, including medicine, car production, banking, manufacturing, agriculture, and marketing, use AI at a fast rate.

This growth is a result of three key technical advancements in recent times: the emergence of big data, the normalization of interactions between humans and machines, and advances in machine learning.

The insurance sector has also been impacted by these advances in terms of newly created business models and capital expenditures employing cutting- edge technology such as artificial intelligence in risk and threat assessment. This frequently covers the dangers connected to the adoption and application of AI itself.

As an alternative, several insurers make investments in game-changing AI technology to improve their operations and risk control. AI will increase the effectiveness of preventative insurance procedures. Insurers may help clients collect, analyze, and interpret their data to prevent illnesses and accidents using AI. The business structure of the insurance sector can change. Thanks to health sensor data, face mapping technology, genetic predictors powered by AI, and AI personal assistants, customers are now better informed about their insurance needs. All of these might result in a reduction in the insurance gap.

Opportunities:

1. Claims Predictions – by employing AI to forecast insurance claims, a client may ask for an explanation as to why their claim was denied. According to reviewed literature, academics used artificial neural networks to deal with health insurance claims.

2. Use of NLP against Phishing – the insurance industry's principal application of NLP in cyber security will be to encourage interactions between people and machines. In order to identify the risk of a phishing attack, insurance firms may use NLP to scan vast amounts of datasets for email conversations. By keeping track of all emails that enter the organization's network, NLP can be used to identify patterns of malicious behavior.

3. Use of AI and ML against DDoS – artificial intelligence and big data help defend firms against DDoS attacks. By comparing network traffic with real-time data streams collected from threat-intelligence sources, correlation engines can spot attack trends. As a kind of cyber extortion, hackers are increasingly using DDoS attacks to force financial institutions to pay hefty sums of money to cease the attacks.

Barriers:

1. Cyber Risks – procedures, such as damage assessment, IT, human resources, and legislative change, all depend on AI. AI systems are extraordinarily quick to learn about petitions, policies, and changes made as a result of those policies. They can also make decisions swiftly. This tactic prompts worries about decision-making accountability, social, economic, and political risks, as well as security.

2. Data Privacy Issues – the enormous potential of technological platforms to obtain and analyze data from a variety of sources – including internet searches, social media accounts, shopping and purchase information obtained from credit card companies – is a threat to customer privacy. The lack of a time restriction on the use of a person's information obtained from a social media account or another source when determining risk is one of the most concerning issues when utilizing AI for data sifting.

3. Discrimination Based on Characteristics – statistics that severely disparage protected attributes that pose a serious threat of bias are not permitted under anti-discrimination rules. Certain legislation, such as the Equality Act of 2010, prevents insurers from using algorithms that can lead to discrimination based on physical characteristics. The potential for indirect discrimination may be negatively impacted by real results of the individualization process created by algorithms.

Emerging AI techniques: impacting traditional risk assessment processes

The primary factor accelerating automation across all industries are machine learning algorithms. However, it has been shown in numerous instances that the use of these algorithms has begun to appear in a variety of cyber-attacks, has improved the effectiveness of those assaults, and has allowed malicious actors to avoid manually addressing statistical analysis issues. The need for strengthening an organization's security posture has increased due to the weaponization of AI and machine learning.

Emerging and state-of-the-art cyber-attack AI techniques

The advancement of cyberattack technology and contemporary techniques is shaping and expanding the field of cyberattacks, exposing cyberspace to a broad range of cutting-edge cyberweaponry with numerous negative effects. Next-generation malware may covertly enter vulnerable and sensitive computer systems while learning from its environment and evolving with new variations thanks to malicious actors utilizing fuzzy models.

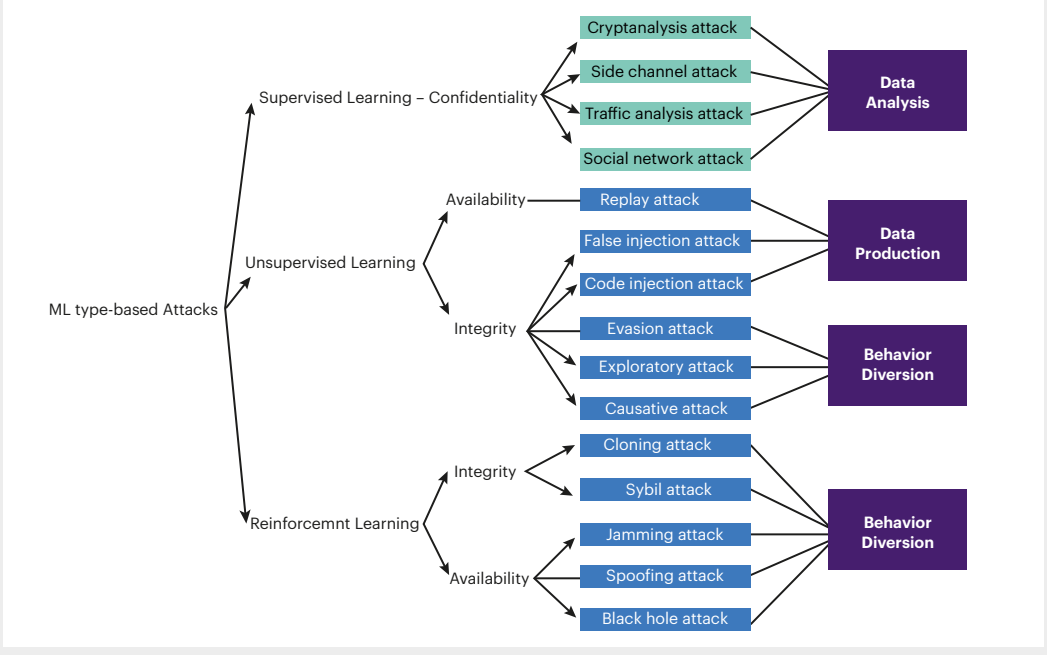
Malicious actors can better learn how computer infrastructures, devices, and cyber defense systems normally work with the use of AI techniques. For example, a malicious actor can identify a key link to targets by gathering architectural, logistical, and topological data about the user's equipment, network flows, and architecture. Massive data collections might provide information about the patterns of targeted attacks that would-be criminals could find using AI. AI's ability to comprehend, unearth, and recognize patterns in massive amounts of facts allows it to be utilized to offer in-depth research and create targeted exploration processes while overcoming human limitations.

As shown below in Figure 1, different types of algorithms can be used to undertake various kinds of cyber-attacks. The figure helps in mapping out the types of algorithms a malicious actor can use to perform a particular attack. It also assists in describing the purpose of the attack, which may be for data analysis, data production, behavior diversion or behavior deduction.

Impact of weaponized AI on insurance industries

Worldwide insurance companies are a target due to their storing copious amounts of sensitive data. Attacks using ransomware and DDoS powered by AI have grown commonplace. Defending organizations from harmful actors has become very difficult due to the rise in the complexity of cyberattacks made possible by AI.

Fig.1: **ML algorithms used in different types of attacks**



Source: WTW

The interruption of services and other similarly detrimental effects are some of the most worrying effects of a successful cyberattack. A cyberattack may result in reputational damage to a company since consumers may stop doing business with them for fear of a potential breach. If companies are negligent in their duties they may face legal repercussions from governmental authorities. Cybercriminals are continually modifying and enhancing the effectiveness of their attacks, placing a strong emphasis on the use of AI-driven approaches.

Lessons for Businesses: Next Stages in Corporate Cyber Resilience

To understand and emphasize where and when disruption may occur – and what it means for certain industry sectors – companies should undertake hypothesis-driven simulations. Pilots and proof-of-concept initiatives should be planned to evaluate not only performance but also to monitor how successfully an organization may perform a certain function within an ecosystem based on data or network intrusions. This work laid out the following recommendations to build organizational resilience within a company:

- •Educating stakeholders on AI and its multiple uses, including threats
- Implementation of a rational strategic plan based on employing technology utilizing analytics from AI investigations
- Creating and executing a comprehensive data strategy
- Training and hiring competent employees who possess technological proficiency, creativity, and a willingness to work in constantly evolving threat environments

The key takeaways for insurers are to recognize that cybersecurity is not an IT problem but a business concern. Enhancing cybersecurity capabilities by effectively implementing AI and ML algorithms to defend networks against sophisticated attacks is necessary. However, insurers will also want to evaluate their present “pockets” of excellence in cybersecurity and ensure that these best practices are disseminated throughout the organization.

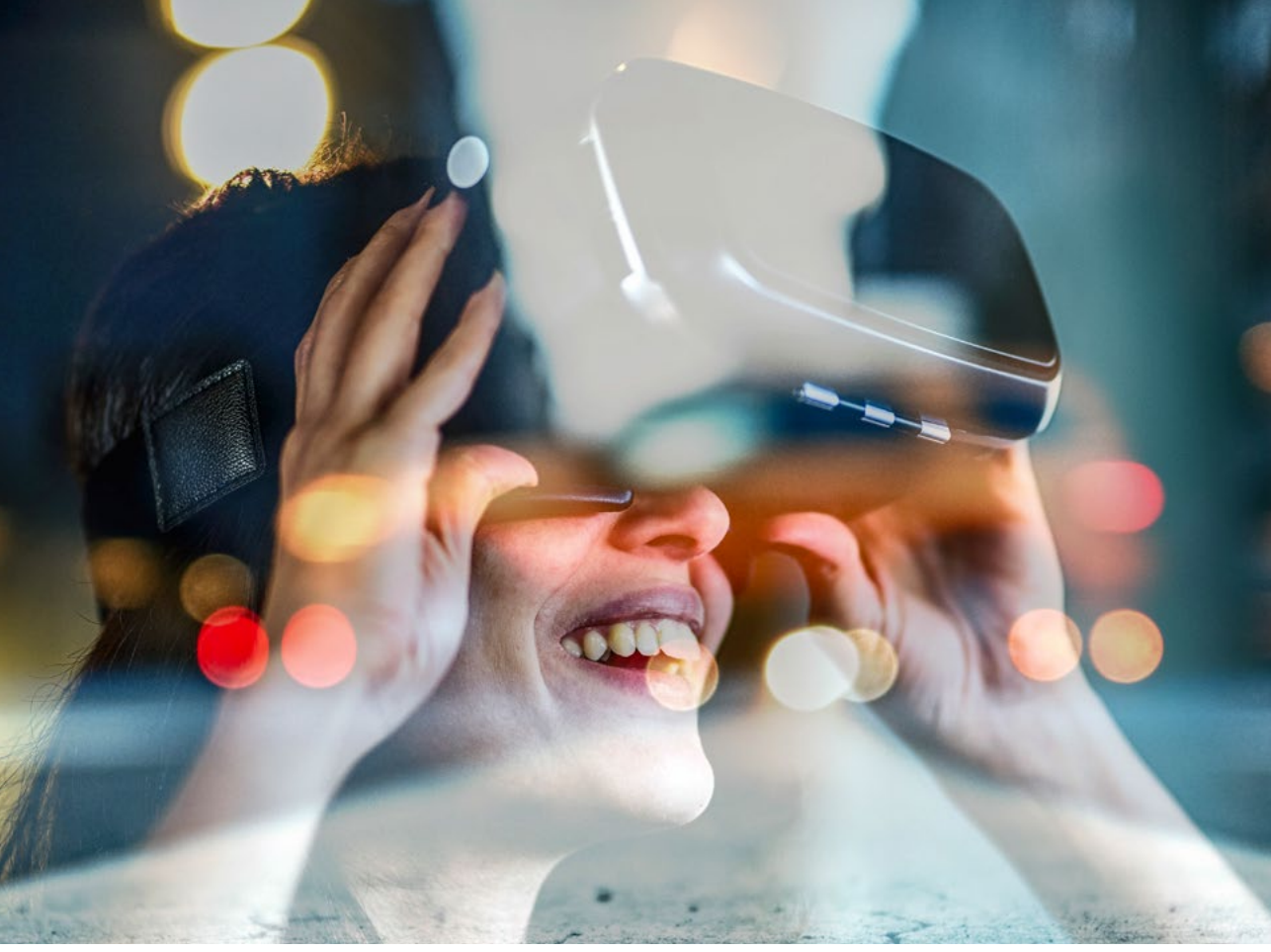
CEOs must collaborate with business executives to best address cyber threats to identify the proper ratio of centralized and decentralized services. Fielding an appropriate response requires the proper framework for robust and consistent cybersecurity. Insurance leaders must carefully evaluate how to ensure their businesses stay prepared, from “red teaming” exercises that mimic the behavior of attackers to increased staff training and regular drills. To manage their risk consistently, insurers must pay particular attention to strengthening their understanding of the ecosystem of third-party players, including independent agents, outsourced service providers, and other non-employees with access to data.

Special feature: TMT Futures Report – workforce transformation and the digital talent crisis

The TMT sector faces a wide range of risks made more challenging by the global pandemic, accelerated digital transformation, geopolitical uncertainty and other factors. Talent gaps have long haunted the industry, particularly when it comes to the so-called 'digital type'.

This problem is set to worsen as rapidly changing technology becomes more complex and expands to new areas of the business, and with competition from wholly unrelated industries now embracing digital, such as department stores and shipping companies, further heating up the battle for top talent.

With the above in mind, and following publication of WTW's TMT Futures Report[1] in August 2021, we continued to work with The Mack Institute's Collaborative Innovation Program (CIP)[2] at the Wharton School, University of Pennsylvania, to dive further into the specific risk issues related the digital talent crisis. Our collective research and interviews with senior executives yielded further fresh insights into the risk issues associated with this key 'megatrend' facing the TMT industry.



Our 2022 TMT Futures Report -Workforce Transformation & The Digital Talent Crisis report[3] is the result of our continued research around the global talent and skills race megatrend which in our view is the most important exposure facing the industry currently and a key link among the broader set of exposures facing TMT businesses.

[1] https://willistowerswatson.turtl.co/story/wtw-technology-media-and-telecommunications-futures-report-risks-on-the-horizon-2021-gated/page/1

[2] https://mackinstitute.wharton.upenn.edu/corporate-partnership/collaborative-innovation-program-partners/

[3] https://willistowerswatson.turtl.co/story/tmt-futures-report-workforce-transformation-and-the-digital-talent-crisis-gated/page/1

Workforce of the future

> **While there is no industrywide model for the workforce of the future, we can make certain projections: it will be increasingly digitally enabled, systematic employee reskilling will become routine, and artificial intelligence (AI) will become an embedded technology across many of the core business processes as companies embrace it to augment, but not replace, human workers.**
>
> TMT Futures Report – Workforce Transformation & The Digital Talent Crisis[4]

Our work with the Mack Institute confirmed our inhouse research that in a digital-first culture[5] there is full organizational alignment that consistently evolves around an integrated digital strategy. Key features include enlightened leadership and human capital management as well as new, agile business models[6] and re-engineered internal processes. We recognise there is no template for what constitutes a digital-first culture that will work for every company, or even narrow industry sector, among TMT and other companies. However, WTW and the Mack Institute jointly found a universal success factor is a clear leadership vision harnessed to highly motivated and skilled employees.

Digital transformation must have a digital-first culture as its outcome, rather than a disconnected collection of technology investments, organizational changes, and a grab for talent. The moving parts must be aligned to achieve optimal business results and constantly fine-tuned to tackle new competitors, changing customer needs, the shifting skill sets and expectations of a restless workforce.

[4] https://willistowerswatson.turtl.co/story/tmt-futures-report-workforce-transformation-and-the-digital-talent-crisis-gated/page/4/2

[5] https://www.wtwco.com/en-US/Insights/2019/08/is-your-company-culture-digital-ready

[6] https://www.wtwco.com/en-US/Insights/2021/12/technology-media-and-telecommunications-futures-report-digitalization-and-technological-advances

Digital First Culture is characterized by the following:

1

Customer experience is a central tenet

2

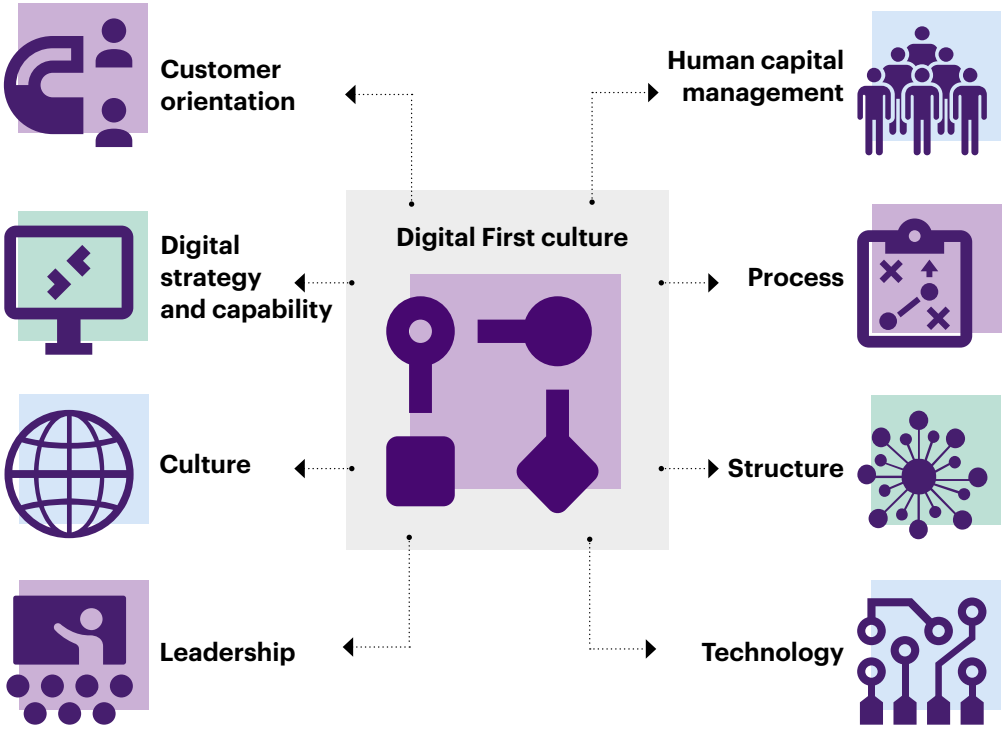
Data is seen as source of value

3

Influence is through insights, not hierarchy

4

Collaboration, iteration, speed, and ecosystems are critical to success



Source: WTW

Reskilling

Digitalization and remote working arrangements have worked remarkably well. But now the initial shock of the COVID-19 pandemic has waned, both companies and their employees are becoming more focused on the long-term implications of markedly new business models and strategies.

Finally, facing global talent shortages, organizations also risk productivity losses if they ignore the imperative to reskill. According to the WEF 2018 Future of Jobs report, 75 million jobs are expected to be displaced by 2022. Concurrently, due to advances in technology and new ways of working, as many as 133 million new roles could be created. However, preparing and reskilling the workforce for these new opportunities will require the CPO's substantial attention; WEF estimates on average, 42% of the skills required to perform a job will shift between 2018 and 2022.

Companies realize they must continuously invest in the latest technologies while keeping an eye open for disruptive competitors and the whims of a fickle client base. From a workforce perspective, TMT companies in particular scramble to the best possible talent, digital and otherwise, while retaining their best employees and equipping them with the skills needed to thrive in a new, often virtual, work environment.

The war for talent that has long engulfed many TMT companies has been worsened by what McKinsey calls a 'labour mismatch'[8] in the U.S., with rising private sector wages despite a persistent talent shortage.

At the same time, the Mack Institute research reminds us employee needs and expectations have changed significantly over the last few years. Many workers like the freedom and flexibility of working from home and resist returning to an office. Others take advantage of digital talent shortages to find new jobs. Many employees in some areas – less technical warehousing or call-in centre jobs, for example – have different needs entirely

[7] https://www.weforum.org/reports/the-future-of-jobs-report-2018/

[8] https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/covid-19-implications-for-business

Conclusion

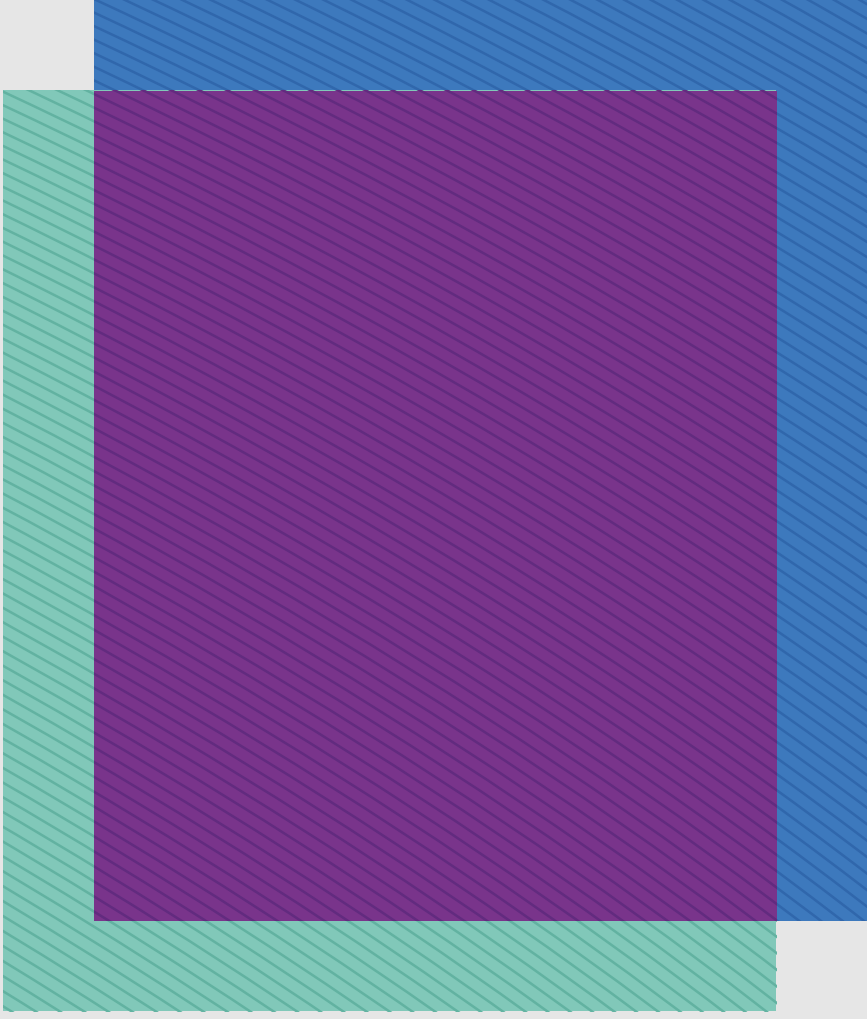
Our work with the Mack Institute identified a variety of approaches companies are taking to achieve a digital-first culture with a nimble, continuously reskilled workforce enabled by AI and other evolving technologies.

As the examples in 2022 TMT Futures Report – Workforce Transformation & The Digital Talent Crisis show[9], there is no one way to achieve a digital-first culture. The culture in any case must reflect leadership vision and behaviour as well as the particulars of a business setting, client base and even geography and other factors.

Although COVID-19 has served as a change accelerant, the pandemic is, to some degree, a distraction. Digital transformation was already underway, and it was ineluctable. Employers simply can't return to factory setting for their postpandemic workforce, nor should they. Now is the time for them to examine their businesses, root and branch, with particular focus on delivering the best possible EX to achieve customer satisfaction and business success.

Our current global business environment represents a rare, exciting opportunity to rethink how work gets done, how jobs have changed and will change, and the upskilling and reskilling pathways needed for a new workforce model to be successful.

[9] https://willistowerswatson.turtl.co/story/tmt-futures-report-workforce-transformation-and-the-digital-talent-crisis-gated/page/1



About WTW

At WTW (NASDAQ: WTW), we provide data-driven, insight-led solutions in the areas of people, risk and capital. Leveraging the global view and local expertise of our colleagues serving 140 countries and markets, we help you sharpen your strategy, enhance organisational resilience, motivate your workforce and maximise performance. Working shoulder to shoulder with you, we uncover opportunities for sustainable success — and provide perspective that moves you. Learn more at wtwco.com.

wtwco.com/social-media

WTW-83951 02/23

wtwco.com