WORLD
ECONOMIC
FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

Trust, Security and Regulation
Dynamic Briefing

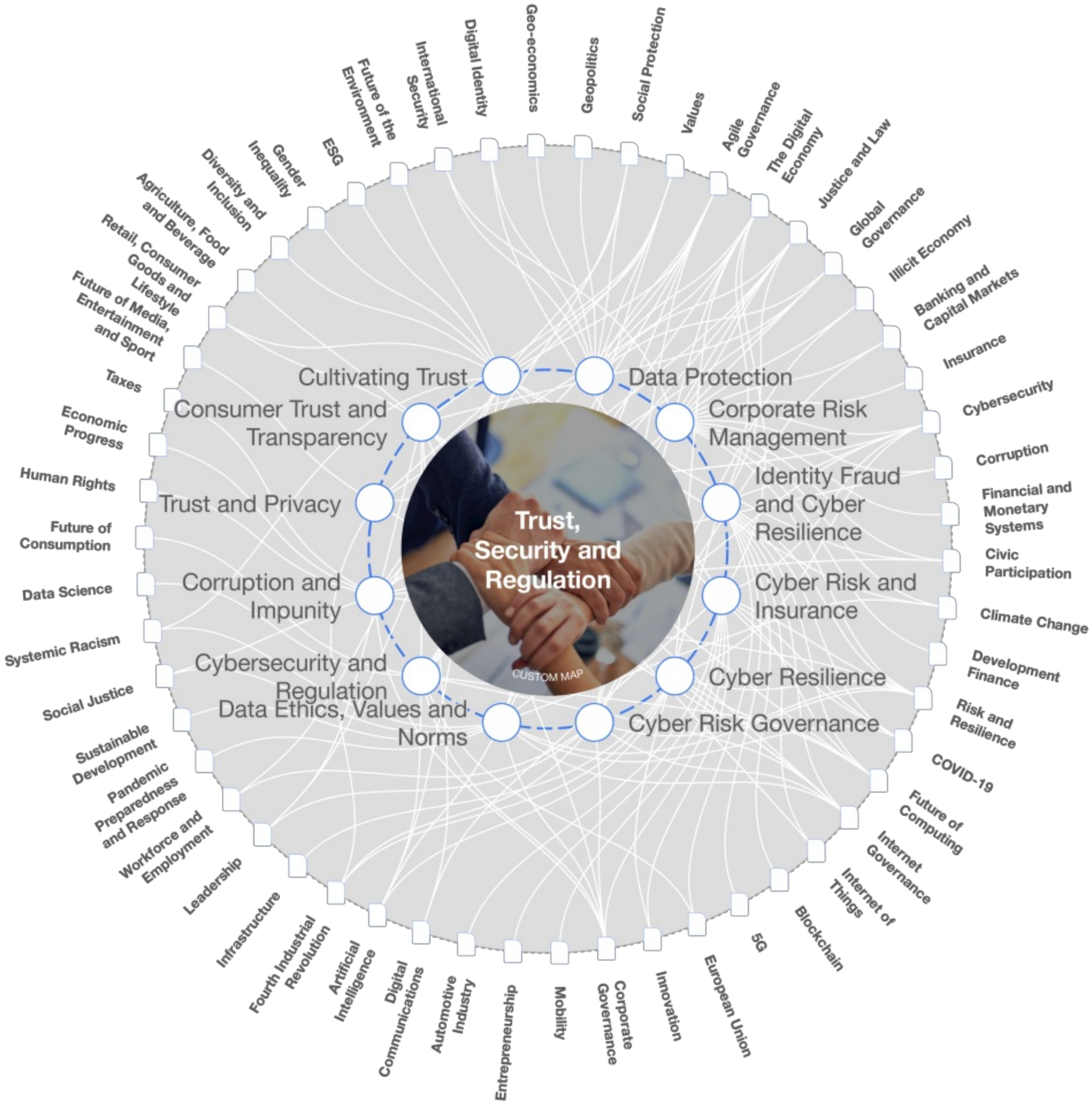
Generated 26 December 2022 for Team Digoshen

Trust, Security and Regulation

Last review on Sun 02 January 2022

About

This dynamic briefing draws on the collective intelligence of the Forum network to explore the key trends, interconnections and interdependencies between industry, regional and global issues. In the briefing, you will find a visual representation of this topic (Transformation Map – interactive version available online via intelligence.weforum.org), an overview and the key trends affecting it, along with summaries and links to the latest research and analysis on each of the trends. Briefings for countries also include the relevant data from the Forum's benchmarking indices. The content is continuously updated with the latest thinking of leaders and experts from across the Forum network, and with insights from Forum meetings, projects communities and activities.



Created by Team Digoshen, licensed for professional use.
© 2022 World Economic Forum

Executive summary

Trust, Security and Regulation Intelligence Map - insights and perspectives curated by Digoshen via World Economic Forum Strategic insights and contextual intelligence.

1. Data Protection

Landmark regulation has not directly led to effective enforcement.

2. Corporate Risk Management

For boards, the volatility of risk scenarios is only increasing.

3. Identity Fraud and Cyber Resilience

The increasing amount of personal data being collected and exploited creates security challenges.

4. Cyber Risk and Insurance

Insurers are underwriting more related policies, as they themselves are increasingly exposed to attack.

5. Cyber Resilience

Accelerating digitization prompts a need for integrated defense, prevention and response.

6. Cyber Risk Governance

The number of corporate boards with a dedicated cybersecurity committee is expected to increase sharply by 2025.

7. Data Ethics, Values and Norms

Data can be deployed to solve global problems and achieve the SDGs, with the right oversight.

8. Cybersecurity and Regulation

The EU has provided a model for the evolution of cybersecurity regulation.

9. Corruption and Impunity

When illicit trade is allowed to flourish, it spawns a culture of impunity.

10. Trust and Privacy

Trust in data-based applications is diminishing, as privacy concerns are not effectively addressed.

11. Consumer Trust and Transparency

In countries where consumer spending is needed to fuel the global economy, trust in businesses is lagging.

12. Cultivating Trust

Responsible corporate governance can create a culture of mutual trust.

Data Protection

Landmark regulation has not directly led to effective enforcement

Data protection has never been more widely discussed. Europe's landmark General Data Protection Regulation (GDPR) was implemented in 2018, and the California Consumer Privacy Act (CCPA) in the US raised the discourse (and the stakes) even further in 2020. As data protection legislation has evolved, it has in many jurisdictions been as much a product of market regulation as of human rights law; data protection law has therefore arguably been a mechanism for redistributing the economic value of personal data. Google and Facebook have recently, in their view, been burdened by this development - as organizations that deeply financially benefit from user data. In legal cases in Europe, such as Maximilian Schrems v. Facebook Ireland Limited, and Google Spain v. AEPD and Mario Costeja González, both organizations have been accused of a lack of transparency. Meanwhile a lack of accountability mechanisms, and frustration with the outsourcing of enforcement to the platform owners themselves, has increased regulatory pressure. So far, evidence suggests the GDPR has increased regulatory burden for smaller companies greatly, while Facebook and Google have yet to see their business suffer as a result.

As the European Union continues to emerge as a regulatory force in data protection, it has renewed a focus on human rights - and on judgements suggesting that commercial entities are responsible for consumer protections including a fundamental right to privacy. However, this renewed focus also risks censorship, due to a lack of directives that take into account the technical particularities of internet services - and the potential impact of applying EU regional law to global infrastructure. Censorship has not been a priority of recent data-protection judgements, however; instead, due to an ambition to counter the dominance of both US authorities and US companies, and to a disparity in regulations, commercial and regulatory power imbalances still pose very real threats to the protection of user data, and to the protection of data subject rights. Intriguing business models have emerged around offering accessibility to enforce rights via data subject access requests (DSARs) - which could possibly lead to a higher quality of data protection standards and "privacy by design" architectures in industries looking to avoid the compliance costs associated with fulfilling such requests.

Related insight areas: International Security, Digital Identity, Geo-economics, Geopolitics, Social Protection, Values, Agile Governance, The Digital Economy, Justice and Law, Global Governance

RAND Corporation

Educating for Evolving Operational Domains

17 November 2022

This report examines how Department of Defense educational institutions are addressing cyberspace and information education, the potential demand for this education, and how the College of Information and Cyberspace can contribute.

Corporate Risk Management

For boards, the volatility of risk scenarios is only increasing

Every organization is confronted with some type of risk - operational, financial, technological, environmental, regulatory - which can have devastating consequences. Effective corporate governance requires continuous and systematic management of all types of risk, both current and anticipated. First, risks must be prioritized, and here the board of directors can play a key role by deciding in what priority they should be addressed, what is to be deemed simply unacceptable, and how they should be addressed from a structural perspective. For example, evidence gathered from the 2007 global financial meltdown indicates that banks with boards that had identified a need to establish a separate risk management committee managed the crisis better than those with integrated committees. The benefits of this type of separation have become only more evident as fiduciary duties have come to include oversight of a broad range of matters, including compliance with international accounting rules and stability measures that require banks to set aside capital in case of potential losses. Implementing a robust risk management system requires the integration of different parts of an organization, including the board's risk committee, internal auditing, finance, legal, and operations.

Increasingly complex and rapidly changing economic, environmental, social, and technological conditions have multiplied potential risk scenarios. Worsening climate change, geopolitical tensions, trade wars, and social upheaval like the protests that spread in Hong Kong in 2019 require corporate governance that is proactive when it comes to identifying risks and addressing them. Determining an appropriate board structure and approach to risk management will depend upon both a company's industry and stage of its life cycle; risk exposure is very different for financial institutions than it is for petrochemical firms. Even within the financial sector, different approaches are required - from insurers exposed to extreme weather events related to climate change, to retail banks making loans to small businesses during volatile periods. Organizations are dealing with complexity and litigiousness like never before, forcing their boards to assess current and past organizational exposure. Still, there are some strategic advantages to taking risks; after all, achieving sustained growth requires some degree of risk-taking. Incorporating risk management into corporate strategy is therefore crucial.

Related insight areas: Illicit Economy, Banking and Capital Markets, Insurance, Cybersecurity, Corruption, Justice and Law, Financial and Monetary Systems, Civic Participation, International Security, Climate Change, Development Finance, Risk and Resilience

Kellogg School of Management

Tesla Deserves an A for Its Financial Management

02 November 2022

Finance & Accounting Nov 2, 2022 Tesla Deserves an A for Its Financial Management Elon Musk should be commended for being in the position to even think about stock buybacks right now. Yevgenia Nayberg In Tesla's earning call last week, Elon Musk said that the company could pursue a $5 billion to $10 billion share buyback.

Identity Fraud and Cyber Resilience

The increasing amount of personal data being collected and exploited creates security challenges

The growing use of digital identities online - in combination with the massive amount of personal data increasingly being collected by governments, businesses, and everything from wearable devices to household appliances - creates significant vulnerabilities. According to the Identity Theft Resource Center, more than 300 million people had their identities compromised between January and September of 2020 alone, and high-profile breaches have included the 533 million Facebook users who had their phone numbers and personal data leaked online in 2021. COVID-19 has accelerated the need for secure digital identity systems, and most organizations are concerned about the security risk involved in increased remote work during the pandemic. Cultivating trust in digital identity relies not only on ensuring privacy but also that data is being issued, shared, and verified in trusted ways through certified authorities. Other approaches for better securing identities and building resilience and trust include keeping data collection to a minimum, alongside disclosure and informed consent. Bolstering digital literacy and helping people better understand the need for password-free, multi-factor authentication can also help.

Security is essential for trusted digital interaction and must be directly embedded in the design of digital identity systems - especially amid the growing use of biometrics. The World Wide Web Consortium, the US National Institute of Standards and Technology, and the Financial Action Taskforce have defined standards for digital identity security, and the app "itsme" uses elements such as multifactor authentication criteria including biometrics, a mobile phone number, and a SIM card linked to the user - along with a personal code. For the Internet of Things, the European Telecommunications Standards Institute has endorsed security-by-design principles - like ensuring devices are not pre-set with passwords, providing a point of contact for issues, and opting into timely software updates. Completely infallible security is impossible, and security is more of a process than a state of being. Stakeholders in all sectors and industries should take proactive design and policy steps to protect digital identities and personal data in order to regain user trust, provide regulatory, certification and control mechanisms, address data breaches, harmonize standards, and encourage digital skills training.

Related insight areas: COVID-19, Future of Computing, Cybersecurity, Risk and Resilience, The Digital Economy, Internet Governance, Internet of Things, Blockchain, Justice and Law, 5G, European Union, Innovation

World Economic Forum

Why we need to regulate digital identity in the metaverse

05 December 2022

Most internet users don't have a digital identity that they own, instead relying on apps like Facebook, Google or LinkedIn for authentication or logging on. However, if users are to move across multiple platforms and the metaverse, they will need a unique digital identity, owned or controlled by them. Standards are needed around creating digital identities, but we must also consider privacy and safety issues around who will regulate them, and how. On the internet, most people don’t have a digital identity that they own. Instead, they deposit information about themselves with a website or app, which then can use that data in several ways, one way being the ability to monetise it.

Cyber Risk and Insurance

Insurers are underwriting more related policies, as they themselves are increasingly exposed to attack

Cyber risk has become a pressing issue both for the insurance sector specifically and for an increasingly digital world generally. According to the World Economic Forum's Global Risks Report for 2019, cyber-attacks ranked among the top 10 risks in terms of both likelihood and impact; the report pointed to massive data breaches during the prior year, the revealing of new hardware weaknesses, and research suggesting the potential use of artificial intelligence to engineer ever-more-potent cyber-attacks. Most respondents in a related survey expected cyber-attacks involving the theft of money and data, as well as disruption of operations, to increase. Insurers are underwriting a growing amount of this risk through cybersecurity insurance policies. According to a report released in 2019, the cybersecurity insurance market was expected to increase annually by nearly 25% until 2024, when it is expected to reach $20.7 billion. Due to its reliance on a proliferation of personal data, healthcare is emerging as the leading target market for cybersecurity insurance; as much as 80% of the data generated by the healthcare industry is estimated to be stored in the cloud.

The healthcare sector's vulnerability to threat has been exacerbated by the broad adoption of telehealth and telemedicine tools - which have only become increasingly necessary during the COVID-19 pandemic. The amplified size and complexity of cyber risks, coupled with a general lack of related historical data, make their pricing challenging for insurers. On the other hand, insurers themselves are increasingly exposed to cyber-attacks - not least as they deploy advanced insurtech tools based on artificial intelligence, big data, and cloud computing. For example, automobile insurers including TD Insurance are offering premium discounts based on information about policyholders' driving habits that is collected in real-time using mobile apps. Insurers must properly manage and maintain such continuously expanding volumes of data, while protecting them from fraud and theft. AI-powered customer service and claims adjustments, implemented for the greater convenience of policyholders, have also led to vulnerabilities that can be exploited by hackers. Ultimately, insurers' transition to cloud computing for quantitative processes, and greater cyber dependency, have increased the risk of outages for entire platforms and networks in ways that can cause losses and disrupt operations.

Related insight areas: Cybersecurity, Digital Identity, Corporate Governance, Innovation, Mobility, The Digital Economy, Entrepreneurship, Automotive Industry, Future of Computing, Digital Communications, Risk and Resilience, COVID-19

Kellogg School of Management

How Experts Make Complex Decisions

01 November 2022

Yevgenia Nayberg Making a simple decision is akin to ordering off a restaurant menu: you evaluate the available options one by one and choose whichever alternative promises to make you happiest or deliver the greatest payoff. When it comes to more complicated choices—say, shopping for a house, devising a business plan, or evaluating insurance policies—identifying the objective “best” option is impractical, and often impossible. to your inbox. Choosing a health-insurance plan, for example, requires estimating the likelihood that you’ll need a biopsy or an appendectomy—a multilayered guessing game sure to be fraught with error.

Cyber Resilience

Accelerating digitization prompts a need for integrated defense, prevention and response

Cyber resilience, or shielding critical systems from hackers or internal failures, is an increasingly important strategic goal in a world of fast, cheap technologies that deliver both unprecedented benefits and risks.

A common denominator for any proper resilience approach is a deep understanding of the risks associated with particular business models. This means that companies must go beyond traditional information-technology planning and make risk evaluation a regular part of their strategy – particularly as they integrate emerging technologies such as artificial intelligence or quantum computing.

Because of the global scope of modern, private sector IT networks, their digital security is a public good. The public sector has its own responsibility to ensure that its institutions also incorporate digital resilience. That's because the risk of the misappropriation of digital public infrastructure, like smart electrical grids or communications devices embedded in roads, will only increase over time. Governments and private actors must work together, to develop new ways to sufficiently protect their digital domains.

Related insight areas: Artificial Intelligence, The Digital Economy, Risk and Resilience, Fourth Industrial Revolution, Internet Governance, Infrastructure, Future of Computing, Cybersecurity

World Economic Forum

New cyber threat landscape spurs shift to zero trust security paradigm

12 December 2022

The world is interconnected like never before but as this digital connectivity expands, so does our vulnerability to cyber attacks. Addressing this increased risks requires a new approach to data security and that is the zero trust model of cybersecurity. Taking a zero trust approach will help protect data and enable organizations to realize the potential of digital transformation. Our everyday life is digitally reliant and interconnected like never before. However, as our digital connectivity expands, so too does our vulnerability and exposure to malicious cyber-attacks .

Geneva Centre for Security Sector Governance (DCAF)

Cyber hygiene course for civil servants

01 December 2022

This course provides a simple, practical, 60-minute training for civil servants of all levels and profiles who, as part of their work, deal with official data and various types of information, and use computers and other IT equipment in the performance of their official duties. It is relevant for existing employees and onboarding new employees. It starts by introducing the basics of cybersecurity and why it is important. Then, it defines what is a hacker and the type of hacking mechanisms they use to attack individuals and organizations. Lastly, it demonstrates the best ways to avoid cyber-attacks and how to stay safe online.

World Economic Forum

Banking can harness cloud technology to hit net zero. Here's how

24 November 2022

As heavy data users, banks can use cloud technology to reduce emissions. The public cloud model is more energy-efficient than banks running their own data centres. Measuring emissions is increasingly a legal as well as a moral imperative. The tone of COP27 could not have been clearer. This is a moment for urgency, to turn pledges and commitments into action.

Boston Consulting Group

Adopting an Ecosystem-First Mindset in Software

10 November 2022

Modern partner ecosystems offer multiple advantages to software firms—but many struggle to build one. Here are five critical strategies for success. As technology becomes ever more crucial for business, companies face many challenges in realizing its benefits. Buying centers proliferate across their enterprise, data security and privacy face increasingly sophisticated threats, and modernizing legacy systems and moving to cloud is a protracted process that becomes more complex each year. By building a robust ecosystem of partners, software firms can better help their customers navigate these challenges—and enjoy a clear competitive advantage.

Boston Consulting Group

Harnessing the Power of Cloud FinOps

07 November 2022

Related Expertise: Digital, Technology, and Data, Artificial Intelligence, Corporate Finance and Strategy Cloud FinOps helps companies manage and get more value from their cloud spending. Getting it right requires robust change management. The cloud ignites digital transformation and growth—but often the spark is dampened because of difficulties in one key area: managing cloud spending. Many cloud FinOps practitioners are thus aware of the gap between where they are and where their cloud FinOps efforts need to be.

Cyber Risk Governance

The number of corporate boards with a dedicated cybersecurity committee is expected to increase sharply by 2025

Governance relies on risk-based decision making as a fundamental means to both drive the efficient use of resources, and to improve confidence in an organization's ability to achieve strategic objectives. All organizations rely on their employees' ability to navigate a world of growing uncertainty, and to dodge threats to their ability to achieve its collective goals. Unfortunately, complex organizations can easily be overwhelmed; each risk demands a distinct analysis and potential investment of additional resources, to respond in ways that adequately reduce exposure. A good governance structure will provide a framework that enables the right managers to make the right decisions, which will help prioritize and allocate resources as needed. All risks don't necessarily require analytic rigour or subsequent investment - immediate hazards like icy sidewalks or commonplace cyber incidents like phishing emails can be addressed at lower management levels. That is not the case for strategic risks like global pandemics or advanced, persistent cyber threats that have the potential to disrupt or damage an organization indefinitely. A structure that effectively prioritizes and adjudicates risks to the right organizational level is required.

Responsibility for risks is typically apportioned in accordance with an organization's willingness to accept them, also called "risk appetite." A risk-appetite statement can be used to direct employees and clarify who has the necessary level of authority to decide how to respond to any given situation. The National Institute of Standards and Technology Special Publication 800-37 addresses the divvying up of risk with a three-tier structure including the organization, the mission, and the system. Meanwhile the ISO 27000 series of standards provides recommendations for the use of policy and organizational structure to reduce risk, and the COSO framework connects governance to culture by highlighting the importance of board oversight, culture requirements, core values, and human resource development. Vigorous, board-level engagement in risk governance is essential for success. Thankfully, boards are increasingly recognizing the importance of cyber risk governance; a study published by Ernst and Young in 2020 found that 81% of board members categorize cybersecurity as "highly relevant," and Gartner researchers predict that 40% of all boards will have a dedicated cybersecurity committee by the year 2025 (currently, just 10% of boards have one).

Related insight areas: Banking and Capital Markets, Leadership, Agile Governance, Workforce and Employment, Corporate Governance, The Digital Economy, Illicit Economy, Internet Governance, Risk and Resilience, Fourth Industrial Revolution

Geneva Centre for Security Sector Governance (DCAF)

#CyberSecMonth is in full swing to build cybersecurity awareness

06 October 2022

Ninety-five percent of cybersecurity breaches are caused by human error. Last year that meant some 22 billion records were exposed by data breaches, with harmful consequences on personal lives and the smooth running of businesses and institutions (World Economic Forum and Risked Based Security). The first step to prevention is to be aware of the risks and learn how to avoid them. For ten years, #CyberSecMonth has offered a full range of tools and resources to do so. Each year in October, hundreds of activities take place across Europe to promote digital security and cyber hygiene, including conferences, workshops, training, and more.

Data Ethics, Values and Norms

Data can be deployed to solve global problems and achieve the SDGs, with the right oversight

The development and deployment of any emerging technology keys on social values, preferences, and ethical norms. It is important for organizations to understand these factors in a local context before formulating how they will govern data and artificial intelligence; in addition to whether local values and norms are adequately reflected, they should seriously consider the interplay between technology and individual rights, and how to put safeguards in place that incentivize responsible and human-centric development. Ensuring the trustworthiness of an organization’s data practices is essential, often for practical reasons; for example, Facebook was sued in the US in 2019, after the Department of Housing and Urban Development alleged the company was violating a prohibition on housing discrimination because its machine learning algorithms functioned like an advertiser that excludes users based on race, ethnicity or religion. Certain foundational elements should be considered at the start of commercial projects: privacy, accountability, safety and security, transparency and explainability, fairness and non-discrimination, human control of technology, professional responsibility, and the promotion of human values. Understanding these in the relevant context is necessary for responsible data use.

By using data responsibly, businesses, non-profits, and governments can better address many of the unprecedented social and environmental challenges we now face - not least current and future pandemics, and environmental disasters aggravated by the worsening impacts of climate change. For example, artificial intelligence can play a significant role in achieving the UN Sustainable Development Goals - one study published in 2020 found that AI can enable the accomplishment of 134 targets across all 17 global goals if its development is supported by the necessary regulatory oversight (though it may also inhibit 59 targets). Some of the levers at hand that can help facilitate the use of data for good include global digital trade, the facilitation of equitable access to data flows, and responsible data collection. Technical elements such as data portability and interoperability are also important. The need to mitigate risks calls for putting firm safeguards in place related to cybersecurity, encryption, risk management, accountability, and overall data protection. Some uses of data and machine learning present particular sets of risks, like privacy breaches and phishing attacks.

Related insight areas: Climate Change, Pandemic Preparedness and Response, Artificial Intelligence, Sustainable Development, Social Justice, Values, Cybersecurity, Corporate Governance, Risk and Resilience, Systemic Racism, COVID-19, Justice and Law, Agile Governance, Internet Governance

Cities Today

London’s first Data Ethicist appointed

14 October 2022

A new Data Ethics Service has been set up to support London boroughs in using data in an effective and trustworthy way.The initiative, launched by the London Office of Technology and Innovation (LOTI), will be led by the first-ever Data Ethicist for local government in the capital, Sam Nutt. The role could become more common in councils as data use advances.

RAND Corporation

Evaluation of the California County Resentencing Pilot Program

28 September 2022

This evaluation of the California County Resentencing Pilot Program seeks to determine how the program is implemented in nine pilot counties and what the characteristics are of a possible candidate for resentencing.

Cybersecurity and Regulation

The EU has provided a model for the evolution of cybersecurity regulation

Government authorities generally require organizations entrusted with data, regardless of industry or sector, to abide by rules intended to protect sensitive, high-value information and other cyber assets. The regulatory environment is fluid, however; it varies in terms of requirements, potential penalties, and execution. The definition of compliance also differs, depending on jurisdiction. The United Nations Conference on Trade and Development divides cybersecurity regulations into four basic categories: data protection/privacy laws, e-transaction laws, cybercrime laws, and consumer protection laws. Regulations aligned with these categories reflect global cybersecurity priorities: 82% of countries have laws governing electronic transactions, 80% formally identify and prosecute cybercrime, 66% address data privacy with specific laws, and 56% have codified online consumer protection. The European Union has served as an enviable model in terms of the evolution of cybersecurity regulation. In comparison with the US, for example, the EU's regulatory environment is generally built upon similar principles related to information-security measures. However, the EU faces additional challenges as it must try to accommodate a more diverse set of cultural, social, and strategic values across the bloc's 27 member countries.

The EU has sought to address cyber risk with policies including the Directive on Security of Network and Information Systems (the NIS directive), the Cybersecurity Act, and the General Data Protection Regulation (GDPR). While the NIS directive obliges member states to develop frameworks for cybersecurity practice, the Cybersecurity Act complements it with a certification framework. The GDPR marks the strongest step taken yet by any developed country to issue requirements for protecting consumer and user information from exploitation. In addition, the EU has established the European Union Agency for Cybersecurity (ENISA) to implement policies and assist member states during incidents. Other countries and regions have made similar attempts to codify rules and cybersecurity best practices, which continue to evolve amid a shifting technology environment. The vanguard of regulators continue to seek to implement ever-stronger reporting requirements, enhanced detection capabilities, data security and disposal rules, and cyber-crime prevention. This trend will persist as long as governments acknowledge the real potential for negative cyber outcomes. Some incidents, like data breaches, may never be meaningfully prevented - even as regulations continue to evolve.

Related insight areas: Agile Governance, Data Science, Global Governance, Corporate Governance, The Digital Economy, Future of Consumption, Future of Computing, Justice and Law, Internet Governance, European Union

Executive Magazine

A weak position in the undeclared cyber war

28 September 2022

We live in a time when hardly a day goes by without hearing about a cybersecurity incident. The need for a safe and secure digital world significantly grew after the… The post A weak position in the undeclared cyber war appeared first on Executive Magazine .

Corruption and Impunity

When illicit trade is allowed to flourish, it spawns a culture of impunity

Organized crime and illicit economies are increasingly prominent sources of political corruption, as criminal networks pour money into parties and forge alliances with officials and their intermediaries. Transnational organized crime generates an estimated $870 billion in annual revenue, and about one third of organized crime groups surveyed by the United Nations have political influence at the local level, according to a report published in 2016 by the Global Initiative against Transnational Organized Crime. Transactional corruption of law enforcement and public officials diverts resources from the state, and increasingly, in countries with poor institutions, the receipt of a bribe is perceived as a right of office - while payment of a bribe is seen as a cost of doing business. This has generated distrust in politicians, distorted markets, undermined public infrastructure, and disengaged citizens. During the 2014 regional elections in Peru, for example, the Ministry of the Interior announced that 124 candidates had links to drug traffickers - yet, 14% of those candidates were ultimately elected, according to the Global Initiative against Transnational Organized Crime’s 2016 report.

Crime and corruption are further facilitated by the decline of stigma associated with illegal acts; illicit activity is regularly used to gain political power, or to buy legitimacy with the public. A lack of law enforcement, penalties, or any deterring government presence at all runs the risk of increasing complicity over time. In Afghanistan, for example, the lack of a state presence is thought to be the most important contributing factor to the rampant opium production in the southwestern provinces of Helmand, Kandahar, Nimruz, and Farah, according to the Global Initiative against Transnational Organized Crime’s report. In many areas of Afghanistan, the Taliban has taken advantage of the lack of state security to become the security provider itself, and its drug-related income - from both smuggling and protecting fields from police scrutiny - has been estimated to be as much as $155 million annually, according to the report. The high-level business and government officials who enable criminal behaviour through neglect or complicity are exacting heavy cost on the rest of us; the annual cost of corruption in the form of bribery and theft amounts to about $3.6 trillion, according to a UN estimate published in 2018.

Related insight areas: Human Rights, Economic Progress, Agile Governance, Social Justice, Risk and Resilience, Corporate Governance, Taxes, Social Protection, Global Governance, Justice and Law, Corruption, Civic Participation

Royal United Services Institute (RUSI)

Corporate Criminal Liability: Lessons from the Introduction of Failure to Prevent Offences

30 September 2022

Corporate Criminal Liability: Lessons from the Introduction of Failure to Prevent Offences Main Image Credit Courtesy of Morakot / Adobe Stock Have 'failure to prevent' offences had an impact on the criminal liability for corporate entities? Executive Summary It has long been difficult for prosecutors in the UK to hold corporates to account for criminal behaviour and, in particular, for economic crime-related misconduct.

Trust and Privacy

Trust in data-based applications is diminishing, as privacy concerns are not effectively addressed

Global dialogue around the governing and safeguarding of personal data is polarized. The often conflicting objectives of governments, businesses and private citizens result in a complicated and often emotional discourse – which hinders informed decision-making.

Personal data is increasingly seen as a pervasive, 21st-century asset class, like a stock or bond. That comes as business models are being built around unprecedented opportunities to create value through the flow of such data. According to the 2014 World Economic Forum report Personal Data: The Emergence of a New Asset Class, trust between individuals, governments and companies is necessary in order to fully unlock its potential.

Yet there is a crisis of trust, as stakeholders struggle to agree upon a personal data framework that is reliable and fair. Existing legal frameworks will prove inadequate, due to the speed of change and uncertainty about appropriate rights and responsibilities. The establishment of effective new frameworks must involve a truly democratic approach, if the public's trust in data governance is to be restored.

Related insight areas: Internet Governance, Cybersecurity, The Digital Economy, Future of Media, Entertainment and Sport, Fourth Industrial Revolution, Values

World Economic Forum

How to develop the global cybersecurity workforce and build a security-first mindset

02 December 2022

As security events rise in number and complexity, the global cybersecurity workforce needs a boost in diversity, training and pathways to cybersecurity careers. Training in soft skills and cloud computing knowledge are the two leading skills gaps in the cybersecurity profession. Free workforce programmes are helping give millions of people access to necessary cloud computing skills for a career in cybersecurity. Advanced digital skills like cloud architecture and software development add an estimated $6.3 trillion annually to global GDP. Cybersecurity is a complex and fluid issue facing every industry today.

Asian Development Bank

Challenges and Opportunities in Teacher Education Reforms

24 October 2022

This brief draws on lessons from Finland, Singapore, Sri Lanka, and Uzbekistan to explore how governments can strengthen training and continuous professional development for teachers to boost their skills and improve student learning outcomes.

VoxEU

Why risks from big tech interdependencies require attention

30 September 2022

The entry of big techs into the financial sector raises significant regulatory questions. An attribute of the big tech business model that has been largely overlooked involves intragroup dependencies and external interconnections. This column argues that the risks arising from these interdependencies require prompt attention by financial regulators. With few specific entity-based rules for big techs in sight, the authors present a set of options presently available to financial authorities that could mitigate the risks posed by the increasingly inextricable links between big techs and finance.

Consumer Trust and Transparency

In countries where consumer spending is needed to fuel the global economy, trust in businesses is lagging

Large emerging markets like India and China, where an expanding middle class is expected to buoy the global economy with growing consumer spending in the coming years, are home to notable lags in public trust among the “mass population” in businesses and government, according to the 2019 Edelman Trust Barometer - a survey of 33,000 respondents conducted in more than two dozen markets. According to the barometer, more than two-thirds of respondents agreed that they might be encouraged to buy products from a company with a good reputation - but unless they genuinely came to trust the company behind the product, they would stop buying it. As global consumers become more connected and empowered thanks to digital innovation, they will only place more scrutiny on businesses. For corporate leaders, this means having to strike the right balance between short-term gains and long-term value creation. According to the Edelman Trust Barometer, one means of winning external trust is by investing internally in employees; 78% of barometer respondents agreed with the idea that the way a company treats its employees is one of the best indicators of its level of trustworthiness.

People have fundamental concerns about the safety and quality of the goods they consume. In China, for example, worries about food and medicine safety have become significant (particularly among wealthier consumers) in recent years, according to a report published by the World Economic Forum in 2018. In addition, these affluent, urban-dwelling consumers in China have particular concerns related to the historical role of fake products in the country, according to the report. Another growing area of consumer concern is related to transparency in supply chains - whether it’s tied to sustainable sourcing or ethical labour standards. In the apparel sector, efforts have been made by the Sustainable Apparel Coalition and Better Work, a collaboration between the UN’s International Labour Organization and the International Finance Corporation, to improve working conditions and sustainability by, for example, introducing standards to measure social and environmental impact. Data privacy is also a serious consumer concern. A relatively small group of companies including Facebook and Amazon (or, in China, Alibaba and JD.com) control large amounts of consumer data - which will present trust issues, as new means of refining and selling that data emerge.

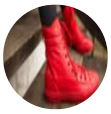
Related insight areas: Internet of Things, Future of Computing, Retail, Consumer Goods and Lifestyle, Internet Governance, Agriculture, Food and Beverage, Digital Communications, Corporate Governance, Values, Global Governance, Leadership, Artificial Intelligence

Cities Today

Barcelona to impose public space tax on delivery firms

15 December 2022

Photo: christian-wiediger-unsplash Barcelona to impose public space tax on delivery firms 15 December 2022 by Christopher Carey Barcelona City Council is set to introduce what it calls a “pioneering tax” to regulate the use of public space by large e-commerce delivery companies.



Harvard Business School Working Knowledge

How Much More Will Holiday Shoppers Pay to Wear Something Rare?

29 November 2022

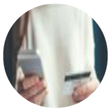
Economic worries will make pricing strategy even more critical this holiday season. Research by Chiara Farronato reveals the value that hip consumers see in hard-to-find products. Are companies simply making too many goods?.

Eco-Business

Reducing the carbon footprint of online retail

22 November 2022

Helped by the Covid-19 health crisis, e-commerce is facing a banner year. According to the 2022 edition of the e-Conomy SEA report released by Google, Temasek and Bain and Co last month, e-commerce in Southeast Asia is projected to end the year as a US$131 billion business, following a 204-per cent growth spurt from US$43 billion in 2019. The report further forecasts that online shopping will continue to expand by 17 per cent annually over the next three years, to be valued at US$211 billion by 2025. Partly as a result of the e-commerce boom, the digital economy in the region is expected to double its greenhouse gas emissions by 2025, figures from the report show.



Harvard Business School Working Knowledge

Will ‘Buy Now, Pay Later’ Push Cash-Strapped Holiday Shoppers Too Far?

21 November 2022

More consumers may opt to "buy now, pay later" this holiday season, but what happens if they can't make that last payment? Research by Marco Di Maggio and Emily Williams highlights the risks of these financing services, especially for lower-income shoppers.

Asian Development Bank

How To Make It Easier for Companies to Participate in Work-Based Training

06 November 2022

How To Make It Easier for Companies to Participate in Work-Based Training To make it easier for companies to participate in work-based training, governments need to mandate, fund, and train institutions to provide such services. Work-based training is more effective in getting young people into jobs than traditional school-based technical and vocation training alone. Many countries in Asia have put in place policies to promote work-based training, yet few companies offer training opportunities that promote the practice. Our research found that practical challenges in setting up work-based training is the main discouraging factor for companies.

Eco-Business

Rise of delivery robots leaves drivers fearful of job losses

18 October 2022

Robot replacement? Delivery robots are predicted to generate about $670 million in global revenues by 2030 - up from $70 million in 2022 - according to ABI Research , an international tech analyst firm. Starship Technologies said its global deliveries tripled in 2021 - its 1,700 self-driving bots made 3 million trips across countries like the United States, Finland, Germany and Estonia. Its robots are pre-programmed with their delivery route, travelling along pavements and using cameras and sensors to cross roads and avoid obstacles. If a Starship bot gets stuck, remote human operators in Estonia can control them and set them on their correct course, said Curtis.

Cultivating Trust

Responsible corporate governance can create a culture of mutual trust

Trust is crucial for the long-term success of companies - especially at the board level. Genuine trust is underpinned by personal integrity, and by putting the interests of the organization (and of society) above those of individuals. Boards need to be able to trust that management will bring full transparency into the boardroom, and that will only happen thanks to shared integrity. There is a strong sense of pessimism about leadership in both the private and public sectors, and anxiety related to job security is high - due to a general lack of training and increasing automation, and not least due to the global pandemic. This threatens to fuel the growth of nationalist and protectionist movements. According to the Pew Research Center, as of 2019 only about one-third of adult Americans had a great deal or fair amount of confidence in elected officials to act in the public's best interests, and less than half said the same about business leaders (attitudes were far more positive when it came to the medical professionals now grappling with COVID-19). In addition to the general public, employees increasingly expect their employers to do the right thing and take action on issues related to inequality, the environment, and climate change.

As people lose faith in their political leaders, it appears that they have higher expectations for CEOs. According to the 2019 Edelman Trust Barometer, more than three-quarters of the general population, or 76%, want CEOs to take the lead on necessary social and economic change rather than waiting for governments to act. While organizations must comply with legislation and regulation on everything from taxes to consumer protection, competition, corruption, and environmental protection, they can also be positively influenced in terms of corporate governance and trust by industry self-regulation and voluntary practices - such as a code of conduct. Most cases of fraud and breach of trust among stakeholders can be traced to corporate governance failures, and so corporate leaders have the ultimate responsibility for creating an organizational culture that supports trust - and ensures that management and employees embody and act on the stated values and mission of their organization. Particular areas of increased social expectations that require the attention of boards of directors include diversity (including gender diversity), transparency, equal opportunity, and eliminating all forms of harassment.

Related insight areas: Diversity and Inclusion, Retail, Consumer Goods and Lifestyle, Agile Governance, Workforce and Employment, Gender Inequality, Values, Leadership, ESG, Civic Participation, COVID-19, Future of the Environment, Artificial Intelligence, Systemic Racism, Social Protection, Climate Change

Eco-Business

Lego and the Toy Makers: How Sustainability Comes to Play Land

14 October 2022

In this report, we aim to research LEGO's ESG performance when compared with other toy makers in the industry by examining their environmental (including carbon emissions), social and governance initiatives. We evaluated LEGO's ESG performance by referring to our ESG framework, which covers 18 initiatives of ESG reporting. Overall, we found LEGO takes the lead in ESG reporting. In particular, LEGO has voluntarily published its sustainability since 2007 and started following GRI (Global Reporting Initiative), and assured its reports by a third party since 2009. We also found LEGO has an ambitious goal of reducing GHG emissions and controlling landfills. However, we do find that its disclosure on pollutants and risk management is missing, and overall disclosures on corporate governance are weaker than other sections.

References

1. Data Protection

- Educating for Evolving Operational Domains, RAND Corporation, www.rand.org

2. Corporate Risk Management

- Tesla Deserves an A for Its Financial Management, Kellogg School of Management, insight.kellogg.northwestern.edu

3. Identity Fraud and Cyber Resilience

- Why we need to regulate digital identity in the metaverse, World Economic Forum, www.weforum.org

4. Cyber Risk and Insurance

- How Experts Make Complex Decisions, Kellogg School of Management, insight.kellogg.northwestern.edu

5. Cyber Resilience

- New cyber threat landscape spurs shift to zero trust security paradigm, World Economic Forum, www.weforum.org
- Cyber hygiene course for civil servants, Geneva Centre for Security Sector Governance (DCAF), dcaf.ch
- Banking can harness cloud technology to hit net zero. Here's how, World Economic Forum, www.weforum.org
- Adopting an Ecosystem-First Mindset in Software, Boston Consulting Group, www.bcg.com
- Harnessing the Power of Cloud FinOps, Boston Consulting Group, www.bcg.com

6. Cyber Risk Governance

- #CyberSecMonth is in full swing to build cybersecurity awareness, Geneva Centre for Security Sector Governance (DCAF), dcaf.ch

7. Data Ethics, Values and Norms

- London’s first Data Ethicist appointed, Cities Today, cities-today.com
- Evaluation of the California County Resentencing Pilot Program, RAND Corporation, www.rand.org

8. Cybersecurity and Regulation

- A weak position in the undeclared cyber war, Executive Magazine, www.executive-magazine.com

9. Corruption and Impunity

- Corporate Criminal Liability: Lessons from the Introduction of Failure to Prevent Offences, Royal United Services Institute (RUSI), www.rusi.org

10. Trust and Privacy

- How to develop the global cybersecurity workforce and build a security-first mindset, World Economic Forum, www.weforum.org
- Challenges and Opportunities in Teacher Education Reforms, Asian Development Bank, www.adb.org

11. Consumer Trust and Transparency

- Barcelona to impose public space tax on delivery firms, Cities Today, cities-today.com
- How Much More Will Holiday Shoppers Pay to Wear Something Rare?, Harvard Business School Working Knowledge, hbswk.hbs.edu
- Reducing the carbon footprint of online retail, Eco-Business, www.eco-business.com
- Will ‘Buy Now, Pay Later’ Push Cash-Strapped Holiday Shoppers Too Far?, Harvard Business School Working Knowledge, hbswk.hbs.edu
- How To Make It Easier for Companies to Participate in Work-Based Training, Asian Development Bank, blogs.adb.org
- Rise of delivery robots leaves drivers fearful of job losses, Eco-Business, www.eco-business.com

12. Cultivating Trust

- Lego and the Toy Makers: How Sustainability Comes to Play Land, Eco-Business, www.eco-business.com

Acknowledgements

- Cover and selected images throughout supplied by Reuters.
- Some URLs have been shortened for readability. Please follow the URL given to visit the source of the article. A full URL can be provided on request.

Continue the experience online

Explore the collective intelligence of the World Economic Forum

In today’s world, individuals and organizations can find it difficult to keep up with the latest trends or to make sense of the countless transformations taking place around them.

How can you decipher the potential impact of rapidly unfolding changes when you’re flooded with information—some of it misleading or unreliable? How do you continuously adapt your vision and strategy within a fast-evolving global context?

Leaders require new tools to make better strategic decisions in an increasingly complex and uncertain environment. The World Economic Forum developed Strategic Intelligence to help you understand the global forces at play and make more informed decisions.

Connect to Strategic Intelligence

Visit Strategic Intelligence on the web or download the Strategic IQ app on your mobile device to learn more.

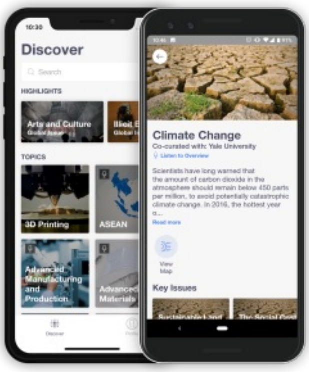
Strategic Intelligence

Strategic insights and contextual intelligence from the World Economic Forum

Explore and monitor the issues and forces driving transformational change across economies, industries, and global issues.

Strategic Intelligence
English
WATCH VIDEO
Highlights
Advanced Manufacturing and Production
Digital Economy and Society
Education, Gender and Work
Environment and Natural Resource Security
All Insight Areas

intelligence.weforum.org



Climate Change

Co-curated with: Yale University

Scientists have long warned that the amount of carbon dioxide in the atmosphere should remain below 450 parts per million, to avoid potentially catastrophic climate change. In 2016, the hottest year o...

wef.ch/si

WORLD ECONOMIC FORUM

Download on the App Store

GET IT ON Google Play

WORLD
ECONOMIC
FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org