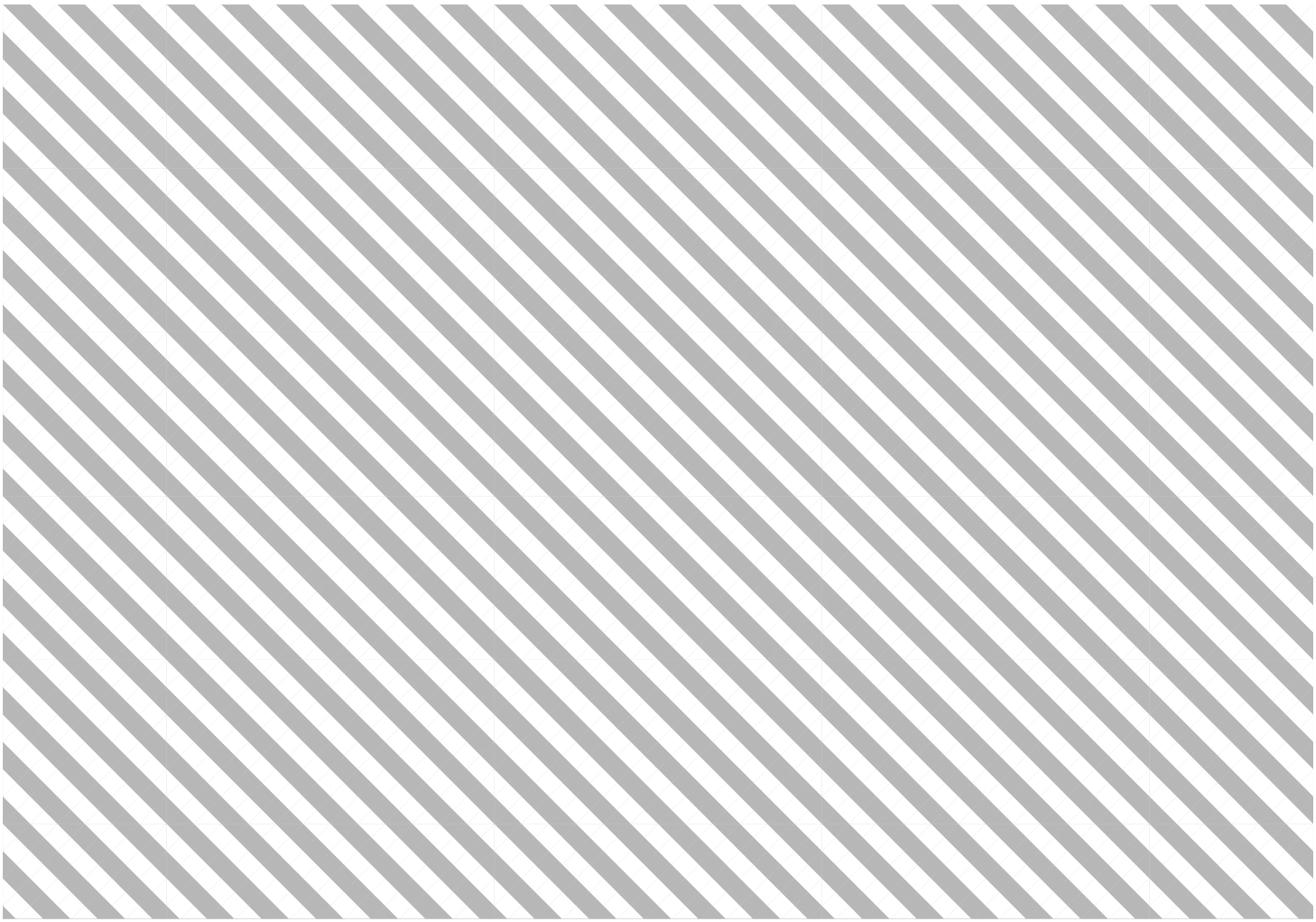
WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

System Initiative on Shaping the Future of Digital Economy and Society

Our Shared Digital Future

Responsible Digital Transformation – Board Briefing



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
Email: contact@weforum.org
www.weforum.org

Contents

Foreword

Derek O'Halloran, Head, Future of Digital Economy and Society Member of the Executive Committee, World Economic Forum

Winston Griffin, Project Collaborator, Seconded to the World Economic Forum by Procter & Gamble

By 2022, 60% of the global GDP will be digitized. Yet today only 45% of people trust that technology will improve their lives. Every sector is beginning to face deep questions about what the implications of this transformation will be.

Previous collaborative research undertaken by industry communities at the World Economic Forum outlined the tremendous benefits that could be gained from this transformation. These include creating significant new economic value, meaningful and rewarding employment, and new products, services and markets that contribute towards sustainability and societal value. At the same time, however, public understanding is growing about the potential risks, in terms of privacy, security and job insecurity.

Digitization is rewriting the social contract – changing the relationship between individuals and the state and individuals and business.

From a business perspective, the first challenge is immediate and existential. Digitization reduces barriers to entry and opens the possibility for new business models that disrupt incumbents. Digitization will ultimately reshape markets, sectors and the role of companies in ways that are yet to become fully clear. Business models will evolve rapidly, and cross-industry platforms and ecosystems are already emerging.

On many issues, business is today being increasingly challenged about its role in society. In the digital context, the responsibilities of organizations as the primary stewards of our data, or as providers of connected devices that we rely on for safety, are equally being called into question. As every company becomes a tech company, these new responsibilities will affect every digitally enabled organization.

What this means is clear: We must develop our understanding and practices along multiple strands at once. We must rapidly engage in transformation and innovation programmes. We must encourage and participate in multistakeholder dialogue on the societal impacts of technology and our role in shaping positive outcomes. And we must improve our individual and collective understanding of the state of play on key technologies today, in order to support good decision-making. In this final regard, boards play a critical role – as they set the direction for their organizations.

We hope this paper will make a useful contribution and be a good starting point for improving understanding, supporting informed decision-making and enabling all organizations to contribute positively to a trusted, inclusive and sustainable digital economy.

Executive Summary

A responsible approach from business will be essential to managing digital transformation. The motivation to achieve this comes from the need to reconcile two forces. On the negative side is concern in the near term over potential liability for enterprises that are not well prepared. And on the positive side, this is a unique moment for enterprises to rise to the challenge, at a time when industries are rewriting social contracts.

The World Economic Forum (the Forum), via its Global System Initiative on Shaping the Future of Digital Economy and Society, is driving the agenda of "Our Shared Digital Future". One of its goals is delivering responsible digital transformation (RDT), and this paper aims to provide a framework on how to think about the impacts from five emerging digital developments of cyber-resilience, data privacy, the internet of things (IoT), blockchain and artificial intelligence (AI).

The target audience for this paper are the boards of all organizations, and the objective is to provide a practical toolkit for use by the "normal board". This potential global audience includes listed and private companies, non-profit organizations and public-service delivery organizations. We hope that government agencies overseeing commercial and economic activities will find insights for policy-making and reach a better understanding of the needs of the business community in terms of regulatory frameworks and the enabling environment.

As part of the work, the Forum ran a consultation with business leaders and regulators during 2018 to explore the topic of responsible digital transformation. This revealed three themes: the large expected productivity gains; the inability of regulatory frameworks to cope with the rate of change; and the increasing role and leadership expected of boards.

The productivity consensus was that digital transformation will represent an unprecedented opportunity to achieve economic gains for society. On the risk side, there was a concern that cyber breaches could lead to a loss of trust throughout all sectors of society. Respondents expected widespread disruption of business models as digital transformation erodes traditional barriers to market entry and generates a new mix of winners and losers. There was a consensus that the process will involve job losses in the short term, but no clear picture emerges on the longer-term impacts.

On the regulatory front, the consensus was that the speed of technological advances contrasts with the length of the regulatory cycles. The rate of change is simply too quick for regulation to keep up – hence the expectation that business needs to step up.

Boards of enterprises have a big role to play. It is important for boards to realize that all companies are now "tech companies" to some degree, regardless of the sector in which they operate. Board members must understand and embrace this digital transformation and become proactive and integrated into what these emerging technologies will mean for operations, product/service offerings, finances, business models and labour. Digital issues must rise on their agendas because the opportunities and risks could be fundamental to the long-term viability of their enterprises.

> "Previously, board membership required a combination of industry knowledge and networks. This is no longer enough. Technical skills required to oversee digital transformations are now modern and specific"

Theo Bouts, CEO, Mobile Division, Zurich Insurance Group

> "Boards will need to change from a 'sitting in the car approach' on digital and data governance to more of a 'hovering over the car approach', to be able to see what is coming around the next bend."

Mats Granryd, Director General, GSMA

> "It will be next to impossible for governments and government policy to react quickly (say within the next three years) to resolve the short-term negative impacts that will arrive with digital transformation. Therefore, it will be up to the incumbent business community to help manage the change. Business leadership needs to embrace the problem and the responsibility to minimize the disruption … Boards need to get aligned with the century."

Deepak Krishnamurthy, Chief Strategy Officer, SAP:

The five digital transformations covered in this toolkit are at different stages but are all interlinked. **Cyber-resilience** is no longer an aspiration, rather it is a basic requirement in operating any enterprise. **Data privacy** issues are already upon us, and complete changes in corporate culture may be needed. **IoT** will be a great accelerator, but it will also compound data privacy and cybersecurity issues, both for good or bad. And **blockchain or distributed ledger technology (DLT)** may prove disruptive to many intermediation-based business models. The challenges of mass **AI** usage are only now starting to emerge and may require a rethink of baseline expectations on what constitutes business accountability.

The narrative structure of the paper includes an overview of each technology; the essential responsibilities for business, government and society; and some tools to help boards focus on vital adaptations within their organizations. Signposts to curated Forum expert papers and useful external reading are also provided.

Toolkit list of board questions:

Foundational

1. Are our breach response plans tested and in place, including plans to deal with reputational risk?
2. Is there a data strategy on what, how and for what purposes we collect data? Are we clear on where and why we collect sensitive data and high-volume personal data?
3. Is there an accounting inventory of all active devices, platforms and systems, with access, detection and remediation plans in place for all our essential systems?
4. Are privacy by design and default and cybersecurity logic built into our front-end innovation?
5. Is our supply chain vetted and working to the same standards?

Principled

1. Are the data collections we use for AI trustworthy, measurable and repeatable, and can we explain how we reach a specific outcome from all our algorithmic decision processes?
2. Does a culture of “algorithmic accountability” and “ethics by design” exist in our organization?

Organizational

1. Are we hiring people with the necessary level of technical mastery and are we investing enough in training?
2. Is the chief technology leader given final accountability?
3. Do we have a culture of human-centredness in our organization?
4. In addition to tracking investments and financial returns from digital transformation, are the societal benefits also being recorded?

And you as a board member

1. Do you deeply understand the business model and the points of vulnerability?
2. Do you as a board have enough collective digital expertise?
3. Do you understand the core principles behind the regulatory framework?

Project Findings

Topic 1: Cyber-Resilience – The Immediate Challenge

Overview

At its simplest, being cyber-resilient means taking measures to prevent and protect against the criminal or unauthorized use of electronic data. As digital transformation gathers pace, cyber-resilience will move up the world's agenda. The number of data breaches is increasing, as is the severity of the attacks. Based on the Gemalto Breach Level Index,[1] the first half of 2018 saw 945 data breaches affecting 4.5 billion records, a 133% increase over the same period last year. More than 90% of events involved unencrypted data and 65% identity theft. A significant number of breaches involved government records. The Forum recently published the 2018 Global Risk report[2] showing the increasing risks to cybersecurity over the past decade. More pointedly a respondent pool of 12,500 companies covering the three largest regions of North America, Europe and EAPAC named digital cyber-resilience as the biggest global risk. Business, government and citizens all stand to lose if we cannot create a safe digital environment to capture the potential gains from the Fourth Industrial Revolution.

Responsibility and call to action of business, government and society

Business: Cyber-resilience requires good housekeeping, as well as a deep and sophisticated network of defences. The primary source of vulnerability is human error, so all enterprises need to **train their employees on digital habits** and basic security protocols to shore up this first line of defence. Businesses need to create a **new cyber-fit culture**. Corporate IT training budgets are increasing,[3] but need further focus, in much the same way that they were made a priority in the 1980s when information technology first arrived. At its simplest level, attitudes to protecting the digital space should match approaches to guarding physical space. Access rights and authentication standards need to be enforced. The essential first objective is to minimize all insider risk. Inter-company behaviour may shift back towards the **traditional "need to know" as a working principle**. Companies should explore using internal data classifications such as secret, confidential, business and public, to increase awareness inside their organizations.

A central inventory of all networked devices and applications is a required second step and all mobile devices may have to be monitored. Organizations need to form and train incident response teams. Very importantly, third-party risk is a concern as supply chains may be vulnerable after decades of outsourcing. Supply systems may need recalibration to ensure vendors reach minimum cybersecurity standards.

At the enterprise level, cybersecurity risks can be reworked into the business model to ensure security by design is a first step. And the management role of the chief information security officer and the cybersecurity team should move from reactive to proactive. A direct reporting line to the CEO should be considered where possible, as well as regular interactions with the board. Extensive breach scenario analysis and risk modelling need to be part of the regular board agenda.

> "The biggest risk is cyber-resilience. And derived from that, the loss of competitive information, and a reputational hit from a breach and/or a significant operational shutdown."
>
> **Jon Moeller**, CFO, Procter & Gamble

Governments: In the absence of global cyber laws or treaties, governments have an enabling role to develop coherent national cybersecurity strategies and transnational and regional treaties, in much the same way as has been done for international trade. They need to ensure that public databases and national infrastructures have the necessary safeguards and establish regulatory frameworks that accelerate the adoption of cybersecurity practices. Law enforcement needs to be standardized and deterrents to cybercrime shared between nations. Enforcement would need to avoid the pitfalls common to white-collar and insider-trading cases. Forward-looking ideas include formalizing the external responsibility of the chief information officer in terms of system integrity – as is the case for the chief financial officer on financial reporting. Governments and business leaders need to work on these ideas in concert rather than in opposition.

> "In general terms, the digital regulatory approach has historically followed the telecom sectorial framework, which has been characterized by an incremental approach. The general sense is that the regulatory bodies are less ready to deal with the transformation and horizontality of the new technologies."
>
> **Fiona Alexander**, Associate Administrator, National Telecommunications and Information Administration (NTIA)

Society: A global educational curriculum needs to teach best online practices and provide early guidance on good housekeeping in managing personal data. Households could manage their digital entry points and control password logic, in much the same way that they organize for physical safety. Individuals can be more aggressive in reporting phishing attacks, and society needs to be proactive and engage in dialogue about practical decisions on common interests in digital safety, security, privacy and trust.

> “The biggest issue for a typical board to focus on is how to become cyber-resilient quickly.”

Brad Smith, President and Chief Legal Officer, Microsoft

Learn more on cyber-resilience
World Economic Forum Report 2017: *Advancing Cyber-Resilience Principles and Tools for Boards.*
World Economic Forum: Our Shared Digital Future.
NIST: The National Institute of Standards and Technology – Guidelines.

Topic 2: Data Privacy – A Universal Issue

Overview

For the first time since the digital age started, we are seeing citizens and enterprises reassessing the use of data. The model of data extraction by business in exchange for services is under strain. New regulations and increasing awareness of the usage of personal data – both the harms and the benefits – are triggering a review of the balance of power and could lead to new contracts.

Data privacy rests on a definition called personally identified information (PII). PII is any information that can be used on its own or with other information to identify a single person. PII can be linked or linkable. Linked information is any piece of personal information that on its own can be used to identify an individual instantly. Linkable information, on the other hand, is information that on its own may not be able to identify a person, but when combined with another piece of information identifies a person.

Regulations make a point of itemizing special categories such as genetic code, biometric data, sexual orientation, children, geolocation, political opinions, trades union membership and health records. Other "more special" categories singled out are children under 13 and criminal/judicial records, both of which require higher level of consents.

The legal framework is changing. In the face of rapid digital evolution, many of the old regulatory arrangements are no longer fit for use. Their inability to cope with the emerging and entangled threats, including privacy and human rights, cybersecurity, consumer protection and even anticompetitive risks, is increasingly obvious. Transition is under way, and while all countries had privacy laws in place, their focus and enforcement has been uneven. The watershed moment was the new European Union framework GDPR (the Global Data Protection Regulations),[4] effective from May 2018. Three broad themes mark a change from the past. First, the EU defines privacy as a human right. Second, it codifies in detail the seven citizens' data rights to include access, rectification, erasure, restriction, portability, objection and automated decision-making (ADM). And third, it formalizes material fines of up to 2% of global sales for issues of accountability and up to 4% of global sales when businesses also fail in their responsibilities to the seven citizens' rights. Excepting the territorial approach favoured by Russia and China, and the relative inactivity at federal level of the United States, the rest of the world is broadly following the EU model. However, despite the detailed legislation making its way around the world, regulators' abilities and agility to use these tools effectively is still undetermined. The risk of businesses having to manage in the face of inconsistent regulatory rules is real.

Current events are showing that some foundational pillars for ensuring trustworthy systems are eroding.

Responsibility and call to action of business, government and society

Businesses, in particular those that interact directly with consumers, will undergo a **sea change in how they seek, manage and process data**. In the short term, business will face issues if they suffer a data breach or if regulators follow up on consumer complaints. Businesses will need to revamp their data governance and embrace a **culture of "compliance by design"**. Policies and procedures will not be enough. Employees can become advocates and a first line of defence. Culture needs to pivot towards a new business attitude that accepts data as entrusted and borrowed rather than extracted or taken. Training and internal certification programmes will help, as will the C-suite showing more public leadership.

Externally, there will be expanded accountability, as businesses that act as data controllers will assume greater responsibility for the supply systems they use for processing activities.[5] Compliance requirements for all vendors will increase and standardize to reflect the increased risk. One possible negative outcome may be increasing concentration on scaled suppliers to the detriment of smaller ones. Similarly, employee engagements may increase "customer vetting" if potential sales involve governments or services with monitoring technology. As employees react to increased monitoring by employers, employee empowerment may manifest itself in this space.

Functional approaches to governance may adjust so that the roles of chief information security officer (CISO) and data protection officer (DPO) gain visibility and the expertise to be effective.

Governments will manage the clash between the exponential growth of personal data and the regulatory push to protect citizens' data. With the EU, Canada, ASEAN and even California at the forefront, regulators are focused on data-policy reform as a means of protecting citizens' rights from an assortment of threats. There is a sense of harnessing a wave of public awareness regarding data privacy, that businesses are abusing the uses of personal data and that previous fines were not high enough to modify behaviour. While this may be the case, regulators must be mindful of balancing their own power with necessary checks. A focus on following the lead of their citizens' complaints will help governments avoid targeting specific companies or sectors. There are dangers of regulatory overlap, as privacy laws, digital protocols, labour laws and age definitions need coordination between countries to avoid unintended impacts to broader public strategy goals. And the toughest challenge for regulators will involve developing dynamic models to keep laws current, laying the groundwork for **regulating outcomes versus a rules-based compliance system** that may quickly become outdated.

> Government must not legislate [on] or regulate the collection of data. This is a futile exercise. They need to focus dynamic legislation on regulating the management of the data.

Mike Gault, CEO, Guardtime: Mike Gault, CEO, Guardtime:

Citizens also have a vital role to play in the emerging landscape. An initial tension point will come with the realization that current language and taxonomy about our personal data is focused on data that is consented, provided or observed. The highlight must move to the **growing importance and volume of inferential data**. The central point is that individuals and institutions have limited control over what "others will know about us". Citizens will be both consumers and producers of data and the new rules will give them extensive data subject rights. Well used, these rights can be a force for good. Consumer complaints will be a mechanism for early alerts and a trend indicator – and the maturity and repetitiveness of consumer feedback will be important. Unlike product or service complaints, which can be easily classified and have protocols in place for remediation, privacy-driven consumer complaints will need to be tabulated in new ways. The impact of emerging consumer advocacy groups with their implied power of litigation will bring new dynamics, potentially affecting the rate of both innovation and global reapplications. As data processing increases scope and deepens personalization, there will be a need for new models of trust and data agency to maintain the working levels of our data-processing systems. This context may see the emergence of a new environment of ratings, reviewers and trusted certifiers.

> Boards may tend to see their digital environment as 'owned' or 'controlled' by the company. And this is not really the case. It needs to be seen as linked and within context.

Jon Moeller, CFO, Procter & Gamble

A board tension point: Balance will be needed between cyber-risk management/avoiding sanctions and the urge to harness competitive growth by exploiting and processing ever larger quantities of personal data. Lack of regulatory standards will generate tension within organizations as they wrestle with "global to local" challenges. Data compliance will differ for legal entity, country and business unit levels. Global policies may need to be tailored and flexed to fit legacy local laws, and productivity-driven scaled solutions may turn into liabilities at the local level.

Taking a bird's-eye view, the point to understand is that as the rate of digital transformation accelerates, the data obtained from inference, as against that from direct consent or observation, will increase greatly. And that brings with it the warning that it will not be the raw data inputs – be they PII or not – that will get an enterprise into trouble. It will be the use to which these insights are put.

Learn more on data privacy
World Economic Forum: *Data Policy in the Fourth Industrial Revolution – Insight on Personal Data*.
EU Summary GDPR.

Topic 3: Internet of Things (IoT) – The Gateway to Automation

Overview

The internet of things (IoT) is the network of physical devices, vehicles, home appliances and other items with embedded electronics, software, sensors, actuators and connectivity that enables these things to connect, collect and exchange data. The growth in connected devices will be exponential and the total number in use is estimated to reach 50 billion by 2020,[6] all made possible by technological advances and dramatic reductions in the cost of connectivity, computing power and storage. Whereas current IoT spending is dominated by the manufacturing sector, with an estimated $189 billion in spending projected for 2018,[7] spending in transportation, utilities and cross-industry applications continue to edge up.

IoT unleashes new opportunities for smart connected products and machines while also enabling the continuous and exponential collection of environmental and user data that can be used to improve business and service performance, thus leading to an ongoing positive productivity loop. Sanjay Sarma of Massachusetts Institute of Technology (MIT) suggests thinking of IoT as a **new design language for business**, with four essential elements. First, there is connectivity that allows remote device operation and data collection. Computation, or intelligence, is the second component. Intelligent systems enable real-time analytics, insight generation, adaptive responses and customization of the user experience. The third component of IoT's design language is recruitment, the ability of devices to directly interact with other devices. The final element is immersion, wherein connectivity, intelligence and recruitment occur automatically, enabling seamless automation of operational processes and user experiences.

IoT is a powerful tool and will change the way in which we work, live and play, buy and sell and interact. It will force businesses to rethink their operations, their products and service offerings to adapt to a new world in which real-time data fuels new efficiencies and opportunities.

Responsibility and call to action of business, government and society

Business: A vital opportunity for business will be cost reductions resulting from greater productivity in all aspects of the supply and go-to-market chain. This applies to business operations and management of physical assets. These are best thought of in two phases. First, IoT increases productivity by improving connectivity and access to real-time data across existing devices or physical assets. These gains are then amplified by expanding out of single-group processes to reach more and more parts of the supply chain. Secondly, the growth phase uses the exponential access to new data to discover unmet needs. The introduction of IoT requires careful attention to business models and financial planning, as productivity gains and new value creation models may need to happen in parallel. In many sectors, for example, IoT is enabling a rapid shift towards pay-as-you-go or subscription of service usage models.

Insight Box

Consumer goods sector: *There is a high degree of competitive exposure to new entrants armed with a switch strategy. Historically, consumption patterns were based on a "first moment of truth" (influencer), then a "second moment of truth" (at retail) and then a "third moment of truth" (consumption). IoT has the potential to move all three steps to a "continuous moment of truth". This effectively reduces the traditional barriers to entry and could affect business models as it changes the economics of trial*.

Risks on the technology and adoption side need to be managed. The 75% failure rate on IoT testing is high.[8] There may be too much focus put on the technology, and not enough on framing the problems that people are trying to solve. Many businesses underestimate the extent of the digital transformation that may be required when real-time data is introduced into otherwise static operations. Early insights show less need for standardized technology and more need for standards on how the data is classified and inventoried. From the technology perspective, it is important not to lock into a single platform to ensure agility and flexibility among platforms. The degree of data growth will also affect the choices of models – from data storage in the cloud only to hybrid models of cloud with home or local data hubs.

> "To the extent that usage of data for better decision-making is the key opportunity, those companies that are low on the digital curve will lose out. This is particularly true given that all companies are in a way tech. The big angle for boards is how this will affect their business model"

Vishal Lall, Senior Vice President and Global Strategist, Hewlett Packard Enterprises

Government: IoT holds the potential to not only fuel economic growth but also drive significant improvements in quality of life. Government has an essential role to play in helping prevent a growing digital divide and ensure that the benefits of IoT reach the communities in which it can provide the greatest benefit. This includes enabling and investing in digital infrastructure such as 5G networks and other wireless technologies to ease public access and adoption of IoT. Another area of opportunity is government's role as potentially the largest implementer of IoT through urban and rural public services. IoT can generate significant productivity gains, service-level improvements and long-term cost savings for the public sector. Government can also help mitigate the risks associated with IoT by establishing regulatory frameworks that support open standards, interoperability, data protections, transparency, network and device security and other best practices in the design and architecture of IoT systems.

Society: Essential responsibilities include creating a heightened awareness of privacy and personal data as well as cybersecurity risk, given the exponential increase in data entry points and the accompanying needs for access and processing. Public education will also be critical to ensure that the public understand both the opportunities of IoT and the potential risks that can be associated with these devices.

> **Tech has been moving faster than government. And government now needs to provide a broad range of new frameworks. Government intervention will be vital to counter increases in inequality. Government will need to help broaden how those benefits from technological improvements are spread**

Brad Smith, President and Chief Legal Officer, MIcrosoft

Learn more on IoT
World Economic Forum Centre for the Fourth Industrial Revolution: *IoT, Robotics and Smart Cities*.
World Economic Forum White Paper: *Principle of Cross-Industry Collaboration and New Business. Sustainable Models for Impact*.

Topic 4: Blockchain – Distributed Ledger Technology (DLT)

Overview

Blockchain is a decentralized and distributed ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all of the subsequent blocks and with the consensus of the network. This gives it the essential characteristic of immutability. It can be private or public. And while it is most commonly mentioned in the context of cryptocurrencies, there may be greater long-term impact in using the underlying block technology. Using the simple format of an email chain, below is a barebones description of how it logically works:

A working definition: "*You (a node) have a file of transactions on your computer (a ledger). Two government accountants (miners) have the same file on theirs (so it's distributed). As you make a transaction, your computer sends an email to each accountant to inform them. Each accountant rushes to be the first to check whether you can afford it (be paid salary bitcoins). The first to check and validate hits 'reply all', attaching their logic for verifying the transaction (proof of work). If the other accountant agrees, everyone updates their file."*[9]

Responsibility and call to action of business, government and society

Business: Blockchain may have significant applications as a distributed ledger, and as a new business model that eliminates the need for a trusted middleperson. Tasks or models that rely on intermediation as their core deliverable may be at risk of upheaval from new technology. From a cyber-resilience perspective, blockchain will offer potential benefits as its distributed nature will eliminate the current need for large centralized data banks, thus lowering the exposure to data breaches.

Business models that are working with digital assets and that want to remove trusted brokers and do not require high transaction speeds or massive storage capabilities may have an opportunity for productivity gains. The business community is exploring tests in health, financial services and supply chains.

Government: There may be potential applications for blockchain in areas linked to standard digital ID usage, and interactions that require certifications may be open to simplification. On the other hand, blockchain's essential characteristics of decentralization and immutability would seem to put it in conflict with the emerging regulatory framework on personal data.[10] For example, some countries are regulating a requirement to ascertain the location and jurisdiction of data, which goes against the decentralized characteristic of blockchain. Likewise, some regulatory frameworks require businesses to be able to determine the controller and the processor of any transaction. There is also the pressing issue of rapid responses to any of the seven codified subject data rights, including the rights to change, access or be forgotten. These situations come into conflict with the DLT immutability characteristic. For all this to work, one side will have to flex. Either blockchain developers must find ways to use blockchain via anonymization of personal data or regulators have to exempt blockchain from some of the new legal demands.

Society: Other than specialized activities involving cryptocurrencies, society has few widespread examples of public uses of DLT. There are narrow early examples such as some public services in Estonia. However, new developments involving DLT technology for storing individual data may lead to a broader attempt to return the internet to a more decentralized and open format, reversing current trends towards closed protocols and data concentration and accumulation in the hands of a few technology companies.[11] Another topic that will have relevant societal impact is energy usage. Current energy usage for the production of cryptocurrencies is not sustainable, but new energy-efficient validation processes are under development. If successful they may accelerate technology adoption.

Learn more on blockchain – distributed ledger technology

World Economic Forum White Paper, April 2018: Blockchain: *Beyond the hype – a practical framework for business leaders*.

World Economic Forum, April 2018: *These 11 Questions Will Help You to Decide If Blockchain Is Right for Your Business*.

NYT Magazine, Jan 2018: *Steven Johnson, Beyond the Bitcoin Bubble*.

World Economic Forum, September 2018. *Building Block(chain)s for a Better Planet*.

Topic 5: Artificial Intelligence (AI) and Machine Learning

Overview

Artificial intelligence (AI) broadly refers to software that is capable of learning and making decisions almost in the same way as human beings. AI enables machines, devices, programs, systems and services to function in a manner that is sensible in light of the given task and situation.[12] Narrow AI is designed to perform one task or a set of specific tasks. General AI is much broader and deals with more layered and complex forms of learning. Machine learning is more accurately understood as one method to achieve general AI, defined as the science of getting computers to act without being explicitly programmed.[13] Deep learning is a particular type of machine learning that uses multiple layers of artificial neural networks to simulate human decision-making. Deep learning has enabled the rise of technologies such as computer vision, natural language processing (NLP) and advanced robotics.

AI is now emerging as an essential accelerator of digital transition because of three factors:

1. digitalization, which has given rise to very large data sets, with the amount of data continuing to grow at an accelerating rate
2. the rapid growth of computing capacity and decreasing prices, which enable the processing of large data sets by an increasing number of users
3. the continuous development of new data-use algorithms

All three factors are enabled by large entrepreneurial investments that have moved AI from the realm of pure science and academic interest closer to mainstream business.

Responsibility and call to action of business, government and society

Business: While AI presents business with an opportunity for significant productivity gains, it also brings a unique challenge. A simple statement that summarizes this is: **AI trained for one purpose cannot produce or be used for another purpose. Doing so would not be responsible or ethical**.[14] Business needs to manage the quality of data to be used for AI analytics. In addition to having no built-in biases, it must be complete, measurable and repeatable.

> **Businesses need to create a data strategy and think about what kind of data will be needed down the road to train the AI that will define their competitiveness in the years to come.**

Marc Vancoppenolle, Global Head of Government Relations, Nokia

Government: At the aggregate level, government will need to look at the risk of AI from two angles. On the one hand, the potential for "misuse" is high, and will be difficult to manage. Risks include use of AI for evasion and detection avoidance. On the other hand, the risk of "missed use" may be even higher for society.[15] Tools and protocols will need to be established so that the safe sharing of large data pools across different elements of society is possible. Similar to cyber-resilience, a potential idea to help regulators and businesses would be the use of a template from the Sarbanes-Oxley framework, by which the CFO and the CEO formally vouch for the integrity of financial statements: similarly, the CIO and the CEO would vouch for the integrity of the AI processes in use. This implied responsibility for algorithmic accountability would travel throughout the enterprise.

Society: Workforce engagement will be critical, both to help design the processes and to feed the machine learning and training re-loop. In parallel, society will need to test the hypothesis that the benefits of technology will open up new areas of human employment. If this is not true, then new social contracts between business and citizens will be required. In the longer term, society may need to evolve its thinking on what constitutes a code of ethics. Existing codes in place today for doctors, engineers or lawyers working in regulated professions face very different scope levels than those that will be required for a responsible digital transformation. There the ethical issue will be how to achieve a balance between specific business gains and the general interests of society. This is many degrees more complex than a doctor's code with regard to the patient, the engineer's with regard to quality and the lawyer's code with regard to the client.[16] Longer-term problems will involve different cultural attitudes about what is considered ethical. In the context of 65% of global AI investment going to China,[17] cultural differences between countries will need managing.

> **The big question is 'What do we want computers to do?' We need to address the issue of how to keep computers accountable to humans. Technology is simply moving much faster than humanity's ability to organize for it.**

> **Managing digital transformation is not only about engineers and computer scientists. It is about engineering AND liberal arts.**

Brad Smith, President and Chief Legal Officer, Microsoft

Learn more on AI
World Economic Forum Centre for the Fourth Industrial Revolution: *Artificial Intelligence and Machine Learning*.

Conclusion

Digital transformation will affect all areas of society, and to reach a sustainable, inclusive and trustworthy outcome, businesses will need to be a force for good. The boards of enterprises have powerful leverage to help manage the transformation and deliver a responsible outcome.

The five topics reviewed in this paper have provided basic guidance on what to look for. The review has also highlighted how interdependent the five topics are.

Providing a **cybersecure** business environment is now a foundational requirement. Businesses that can quickly become compliant with the new **personal data** regulations, while at the same time moving their organizations to a culture that treats data as borrowed, and then rapidly shift their future focus from the collection of data to the use of it, will maintain the trust of their customer base. **IoT and automated decision-making** will be rapid and scaled amplifiers of data collection, increasing opportunities for growth while raising the overall risk to the enterprise and to society. **Distributed ledger technology** is not yet proven, but it has the potential to affect intermediary-dependent business models. And the emergence of **AI and machine learning** may require a rethink of the social contracts that underpin business.

Boards of enterprises will come to realize that there is no separate digital economy, there is only one economy that is digitalizing at varying speed.[18] This perspective highlights the expectation that boards should demonstrate knowledge of these technologies, but also underscores that true added value will come from boards' ability to see the impacts on the entirety of their business model.

While all of these emerging technologies have concerning downsides, they also promise significant upsides. Each of the emerging technology overview sections was followed by a section subtitled "Responsibility and call to actions of business, government and society" for a reason. While the overall focus of the paper is on how boards can help business deal with the transformation, governments and citizens also have vital roles to play.

Regulators and market-enablers face distinct challenges. There is now evidence that the previous logic of "government goes long and business goes short" is no longer fit for use as an operating framework, and that some sort of dynamic regulatory capability must evolve. As users of these technologies, governments can move quickly to capture gains in productivity and offer improvements in all public services. They can also help prevent a growing digital divide and ensure that IoT reaches the communities where it can provide the greatest benefit.

Citizens also have vital roles to play as they engage with these emerging technologies. Adopting a code of good digital conduct, developing strong personal digital-security habits, exercising new data subject rights fairly and engaging responsibly with businesses on customer complaints will be essential. Together, these behaviours will help create a level of digital citizenship capable of influencing the journey to deliver a responsible transformation.

This paper has attempted to strike a balance between different sources – using the findings from recent business cases, taking insights and forward-thinking from the expert centres at the Forum, and sharing the guidance from external business and society leaders drawn from the consultation process. The focused board-level questions are a good place to start, and the additional readings will be updated periodically to keep the document platform current.

Contributors

Companies and policy-makers contributing to the consultation

Mats Granryd, Director General, GSMA, and member of the DES Stewards Committee
Brad Smith, President and Chief Legal Officer, Microsoft
Jon Moeller, Chief Finance Officer, Procter & Gamble
Mike Gault, Chief Executive Officer, Guardtime
Fiona Alexander, Associate Administrator, US National Telecommunications and Information Administration
Vishal Lall, Senior Vice President and Global Strategist, Hewlett Packard Enterprises
Deepak Krishnamurthy, Chief Strategy Officer; Rogerio Rizzi de Oliveira, Senior Vice President, Corporate Strategy, SAP
Marc Vancoppenolle, Global Head of Government Relations, Nokia,
Theo Bouts, Chief Executive Officer, Mobile Division; Daniel Englberger, Group Chief Transformation Officer; Francis Bouchard, Group Head of Communications and Public Affairs, Zurich Insurance Group
Clayton Daley, previous board member, Starwood Hotels & Resorts
Werner Geissler, board member, Goodyear
Dimitri Panayotopoulos, board member, Logitech

This paper has been written with support from the following World Economic Forum projects: Global Initiative Shaping the Digital Economy and Society, Data Privacy and Policy, Centre for Cybersecurity, Internet of Things, Blockchain and Distributed Ledger, Artificial Intelligence and Machine Learning.

A particular thank you to the following Forum staff their contributions and guidance:
Derek O'Halloran
Mark Spelman
William Hoffman
Jeff Merritt

General Principles and Glossary

General principles of GDPR compliance – eight steps

1. **Legal basis for PII processing**: To ensure an entity is using data lawfully, fairly and transparently. Processes involving PII need to be based on contract fulfilment, consent or legitimate interest.
2. **Data collection**: Data should be collected only for specific, explicit and legitimate purposes and must not be further processed.
3. **Data minimization**: Sought data must be relevant only to what is necessary for processing.
4. **Data accuracy**: Stored PII must be accurate and kept up to date.
5. **Storage limitation**: Data must be stored for no longer than is necessary for the purposes for which it is processed.
6. **Integrity and confidentiality**: Organizations must provide security to protect against unauthorized or unlawful processing and accidental loss, destruction or damage. There can be no data breaches.
7. **Third-party vendor ecosystem**: As data controllers, there is accountability for all of the above.
8. **Compliance by design**: Data-protection features are built early on into an innovation plan.

Glossary of key terms

– Controller vs processor: The controller determines the purposes and the means for the processing. The processor processes PII on behalf of the controller.
– Profiling: Use of automated decision-making (ADM) on processed PII first-, second-, third-degree data.
– Processing: Work on personal data. Includes collection, structuring, storage, adaptation, transfer.

Endnotes

1. Gemalto Index, “Data Breaches Compromised 4.5 Billion Records in First Half of 2018,” 9 October 2018. https://www.gemalto.com/press/pages/data-breaches-compromised-4-5-billion-records-in-first-half-of-2018.aspx. Accessed 14 December 2018.

2. World Economic Forum, *The Global Risk Report 2018*, 13th edition.

3. Bersin, Josh, “Spending on Corporate Training Soars: Employee capabilities now a priority,” 4 February 2014. https://www.forbes.com/sites/joshbersin/2014/02/04/the-recovery-arrives-corporate-training-spend-skyrockets/#24ba08b9c5a7. Accessed 14 December 2018.

4. See General Principles of GDPR compliance – eight steps. IAPP International Association of Privacy Professionals “Operating Principles for GDPR compliance”.

5. See GDPR glossary of key terms.

6. Nordrum, Amy, “Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated,” IEEE Spectrum, 18 August 2016. https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated. Accessed 14 December 2018.

7. I-Scoop, “Internet of Things Spending 2020: IoT Industry Drivers and Spenders.” https://www.i-scoop.eu/internet-of-things-guide/iot-spending-2020/. Accessed 14 December 2018.

8. Chan, Benson, “IoT Projects Have a 75% Failure Rate,” IoT for All, 22 June 2017. https://medium.com/iotforall/iot-projects-have-a-75-failure-rate-ce8101432c25. Accessed 14 December 2018.

9. Deloitte, “Blockchain Explained … in Under 100 Words.” https://www2.deloitte.com/ch/en/pages/strategy-operations/articles/blockchain-explained.html. Accessed 14 December 2018.

10. International Association of Privacy Professionals, “Is Blockchain Incompatible with GDPR?”.

11. Johnson, Steven, “Beyond the Bitcoin Bubble,” *The New York Times Magazin*e, January 2018.

12. Centre for Information Policy Leadership, First Report: AI and Data Protection in Tension, October 10 2018. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ai_first_report_-_artificial_intelligence_and_data_protection_in_te....pdf. Accessed 14 December 2018.

13. *First Report: AI and Data Protection in Tension*.

14. Satya Nadella, CEO, Microsoft.

15. Point taken from recent UN forward-looking guidance.

16. Carson, Angelique, “Should the Privacy Profession Adopt a Code of Ethics?” International Association of Privacy Professionals, 28 February 2017. https://iapp.org/news/a/should-the-privacy-profession-adopt-a-code-of-ethics/. Accessed 14 December 2018.

17. World Economic Forum, “Meet China’s 5 Biggest AI Companies,” 20 September 2018. https://www.weforum.org/agenda/2018/09/the-top-5-chinese-ai-companies/. Accessed 14 December 2018.

18. Gillian Tans, CEO, Booking.com.

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