IMD Faculty

Georges Haour
Emeritus Professor of Innovation Management and Technology Commercialization

Peter Vogel
Professor of Family Business and Entrepreneurship
Debiopharm Chair of Family Philanthropy

Guest Contributors

Professor Benoît Morel
Cybersecurity
Carnegie Mellon University

Professor Solange Ghernaouti
Director of Swiss Cybersecurity Advisory and Research Group
University of Lausanne

Dr Sébastien Ziegler
President of the IoT Forum and Director of Mandat International

Professor Carmela Troncoso
Tenure Track Assistant Professor
EPFL

Isabelle Borfiga
Data Officer
McDonald's France

Dr Sławomir Kukliński
R&D Expert
Orange Labs Polska

Research & Development

Karine Avagyan
Michelle Perrinjaquet

Senior executives from 25 companies recently gathered in Lausanne to attend an IMD Discovery Event on how the digital revolution is impacting their businesses and to discover the opportunities and threats of this digital tsunami.

Discovery Events are exclusively available to members of IMD's Corporate Learning Network. To find out more, go to www.imd.org/cln

The digital tsunami: How it impacts your business

The "digital tsunami," with its virtualization of networks, internet of things (IoT), big data and analytics, robotics and artificial intelligence (AI), is impacting all industries and companies. Old business models are challenged, communication technologies are promoting disintermediation, the job market is undergoing fundamental shifts, and companies face the urgency of reinventing their business models to become agile in a new digital reality. Experts from academia and industry came together to discuss the "lights and shadows" of the brave new digital world.

Cybersecurity

Professor Benoît Morel pointed out that although the digital revolution can be an irresistible force for good, the potential for collateral damage is deeply worrying. To sustain the disruption and not lose their competitive edge, businesses need to consider new functionalities and take advantage of existing as well as emerging technologies, such as CSS, HTML5, G5.

Nevertheless, new functionalities bring about new vulnerabilities. Professor Morel cited several recent cases of cybersecurity breaches, including Equifax and SEC, which were compromised in 2017. To cope with the growing risks related to digitization, businesses have to develop a cybersecurity mindset and foster a culture that goes beyond a piece of engineering to nurture real internal expertise instead of depending on external experts.

Professor Solange Ghernaouti stressed that digitization means datafication, and more data implies higher risks that can impact all levels, not only individual and institutional but also national and international. Cybercrime constitutes a lucrative economy fostered by the Dark Web, the availability of cyberweapons, human vulnerability and opportunity. In some ways, the internet could be considered a crime enabler. Professor Ghernaouti outlined seven types of cyberthreats: cyberincivility, cybervandalism, cyberdeliquency, cyber-criminality, cyberespionage, cyberterrorism and cyberconflict.[1] However, she stressed that cyber risks are not limited to criminal behavior, they can also occur as a result of human error or even a natural disaster. These should all be critical components of a company's overall risk management strategy, translating into operational security.

Both speakers concluded that it is not possible to ensure the complete protection of IT systems from cybersecurity threats; all companies can do is learn how to mitigate the risks while keeping their IT systems efficient and operational.

Privacy by design

As emphasized by Professor Carmela Troncoso, with the growing availability of data and shared infrastructure, privacy is becoming a paramount concern. By linking the available data from all intelligence-based platforms and applications, such as social media, entertainment, e-commerce, etc., an efficient surveillance infrastructure could be built to monitor people. As long as the combined records are anonymized it is not a problem, but if they are in the form of personally identifiable information (PII), it could be dangerous.

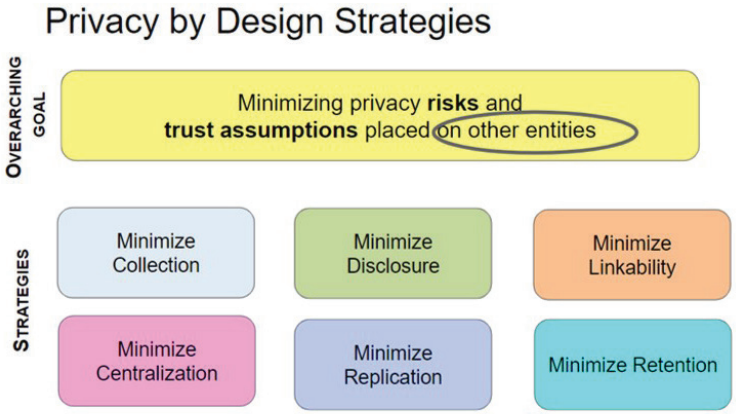
Recent Major Data Breaches

Equifax. In September 2017, Equifax announced a massive data breach of personally identifiable information on over 148 million people. The US Government Accountability Office confirmed that a single internet-facing web server with out-of-date software led to the breach, which went undetected for 76 days. Failure to use well-known security best practices and a lack of internal controls and routine security reviews were identified as the root causes behind this breach.(2)

SEC. In September 2017 the CEO of the Securities and Exchange Commission (SEC) admitted that a year earlier hackers had accessed its corporate disclosure database (Electronic Data Gathering, Analysis, and Retrieval system or EDGAR). In particular, they were able to access non-public information (confidential market listing plans and non-public drafts of proposed rules by stock exchanges) through a software vulnerability in part of the SEC's EDGAR system for test filings. The SEC said the vulnerability was patched promptly and it immediately began an investigation.(3)

Aadhaar. In 2018 India's centralized biometrical identity database Aadhaar, containing over 1.2 billion records and controlled by the National Critical Information Infrastructure Protection Centre, was compromised. According to a report by HuffPost India, a malicious software patch sold on WhatsApp for Rs 2,500 (around $35), allowed unauthorized persons anywhere in the world to generate Aadhaar numbers. Vulnerability is intrinsic to the technology choice made at the start of the Aadhaar program, and the fix would require fundamental change in its structure.

Professor Troncoso's six privacy-by-design strategies – minimizing data collection, centralization, disclosure, replication, linkability and retention – are aimed at reducing privacy risks. The European Electronic Toll Service's electronic toll pricing system is an example of a successful privacy-by-design project, whereby entities and data are classified into two domains – a user domain with location, personal and billing data, and a service domain containing encrypted records that are unidentifiable by the toll authority.



Professor Troncoso concluded that to build successful privacy by design, companies need to shift their mindset from wanting to have all the data, then reducing it to the data they can collect and process, to "the PhD approach" that starts with identifying the necessary data for the specific goal and then collecting that and other related data. In all cases, privacy goals should be clearly identified and evaluated using a probabilistic approach.

Addressing IoT challenges and opportunities

In his presentation, Dr Sebastien Ziegler spoke about several technological enablers of the IoT part of the digital revolution, such as artificial intelligence, nanotechnology (that accompanies sensor development and deployment), IoT – cloud integration, edge computing; 5G and network slicing, IPV6 and multi-protocol integration or device gateway.

Dr Ziegler presented two particularly interesting IoT platform projects: 1) the IoT Lab, a sort of crowdsourcing research platform that connects around 32 European Testbeds into a Testbed as a Service, a common platform where people can connect and run experiments online from remote locations; and 2) SYNCHRONICITY, an IoT platform where cities and businesses develop shared digital services to improve the lives of citizens and grow local economies. This platform combines open data (collected and stored from numerous sensors placed in public areas), data analytics, shared applications and services. So far the project connects eight European cities, as well as three cities from other countries – the US, Mexico and South Korea.

Network virtualization and slicing: New horizons for communication technologies

Sławomir Kukliński presented the historical development of communication technologies and spoke about the current challenges they are facing. The biggest challenge for current mobile networks is the rapid growth in mobile data traffic – it has grown tenfold during the last five years, and the trend is set to continue. In addition, there is a rising need for wide coverage and very high reliability to service IoT, including industry 4.0, drones and automatic vehicles as well as remote healthcare operations (like remote surgery).

In order to solve these challenges, a new communication technology concept – network virtualization and slicing – is being developed. It assumes a combination of cloud computing and mobile network, based on the shared physical infrastructure. This concept is still in the conceptualization stage but will definitely call for new business models. Companies will be able to provide services in the virtual infrastructure at a very low cost.

From data to digital business model

How do companies adopt their business models to embrace and use digitization and IoT? Professor Peter Vogel explained that while the amount of data is growing exponentially, driven by a rapid increase in the number of connected devices, the vast majority of data is just being collected but not being used. To make better sense of the data they collect, companies should introduce dynamic links between various pieces of data, analyze it, infuse it with theory, and only then implement changes and keep track of the outcomes. Data analytics has become an indispensable part of business strategy in successful companies, and a growing number of companies have started to use prescriptive models and cognitive machine learning tools.

To make better sense of the data they collect, companies should introduce dynamic links between various pieces of data, analyze it, infuse it with theory, and only then implement changes and keep track of the outcomes.

Companies can and should leverage integrated "smartness" (augmenting their products with sensors) via connectivity and analytics to develop and deliver customized digital services and thus premiumize their products. John Deere followed this strategy. By integrating a variety of sensors in its equipment, collecting and analyzing the data, it has transformed itself from a tractor manufacturer into an agricultural services platform.

Yet before a company starts integrating digitization and data analytics into its business model, it first needs to understand what value it will be creating through added digitization and what the new business model will look like. It has to be clear who its target customers are, what exactly it can offer them, how the value it promised will be delivered to them and how it is planning to make money on this. In other words, a company should clearly understand and define its value proposition, value chain and revenue model.

Big Data Is Getting Bigger

According to a report from IDC,[4] the "global datasphere" will grow ten times by 2025, and the following five trends will prevail:

- Nearly 20% of the data will be critical to our daily lives and 10% of that will be hypercritical.
- More than a quarter of data will be real time in nature, of which 95% will be real-time IoT data.
- An average connected person will interact with connected devices nearly 4,800 times per day.
- The amount of the global datasphere subject to data analysis will grow by a factor of 50 to 5.2ZB.
- Almost 90% of all data will require some level of security, but less than half will be secured.

Source: IDC report "Data Age 2025" https://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf

How to Include More Intelligence in an Existing System: The Case of McDonald's France – Isabelle Borfiga

Although McDonald's was founded in 1940, the fast-food chain opened its first restaurant in France around 39 years ago. The McDonald's France unit, represented by over 1,400 restaurants and 194 McCafés operated by 320 franchisees, generates just under a quarter of the global $22 billion revenues. McDonald's France has pioneered the digital revolution in the company with the development of various digital tools, such as kiosks (introduced by a French operations team in 2003), a mobile app (introduced in 2012), a dedicated website, a loyalty program, campaigns and online delivery.

A new way of using data was recently introduced in McDonald's France, starting with business understanding followed by data understanding. The next steps include data preparation (which can consume up to 80% of the data science team's time), data modeling (which depends on KPIs and is aimed at understanding and/or predicting the data) and evaluating the models (in conjunction with business understanding). Then comes the often-missing stage of deployment, i.e. creating dashboards and making sense for the end user.

The recent integration of the European GDPR requirements has been a positive experience, bringing together the commercial, financial, legal and technical IT parts of the company to fruitfully collaborate and complement each other.

The new challenges faced by McDonald's France include monitoring stores in real time, industrializing rollout, improving the supplier management process, developing predictive maintenance and preparing for IoT.

Key takeaways

Although the digital tsunami is affecting all spheres of our lives, businesses can take measures to mitigate the possible risks associated with it while still embracing its huge potential. To prepare for the upcoming challenges, companies should consider the following:

- The implicit assumption "the more data the better" should be revised. Instead, companies should answer the following four questions:
  - What data is being collected but not capitalized on?
  - What are the potential sources and types of new data that could be collected?
  - How can value be created from all the available data?
  - Who are the main consumers and benefactors of this value?
- Monitoring current and emerging technologies should become an essential part of business intelligence. Yet when deciding which technology to use, companies should focus on their own needs and goals rather than simply using the same technology as the competitor.
- Top management and boards should be educated on disruptive technologies, and the opportunities and threats they bring to the company.
- To increase the efficiency of data analytics and cybersecurity measures, companies should educate their employees and especially engineers to understand business, its language and needs.

Most importantly, companies should understand that the challenges of successfully leveraging the digital transformation for business success, as well as mastering the cybersecurity risks are not limited to IT specialists. Instead, these challenges require a fundamental shift of the organizational culture that implies efficient collaboration between IT and all other departments and functions affected by the digital revolution.

References

(1) Solange Ghernaouti. "Cyberpower, crime conflict and security in cyberspace." EPFL press – CRC pres, 2013. https://www.ppur.org/produit/625/9782940222667/Cyber%20Power%20?search_text=Ghernaouti

(2) Glenn Fleishman "Equifax Data Breach, One Year Later: Obvious Errors and No Real Changes, New Report Says", Fortune, September 8, 2018 http://fortune.com/2018/09/07/equifax-data-breach-one-year-anniversary/

(3) What we know and don't know about the SEC hack" Reuters, September 21, 2017 https://www.reuters.com/article/us-sec-cyber-q-a/what-we-know-and-dont-know-about-the-sec-hack-idUSKCN1BW2RN

(4) IDC report "Data Age 2025" https://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf