Cybersecurity (finally) leaves its technical ghetto

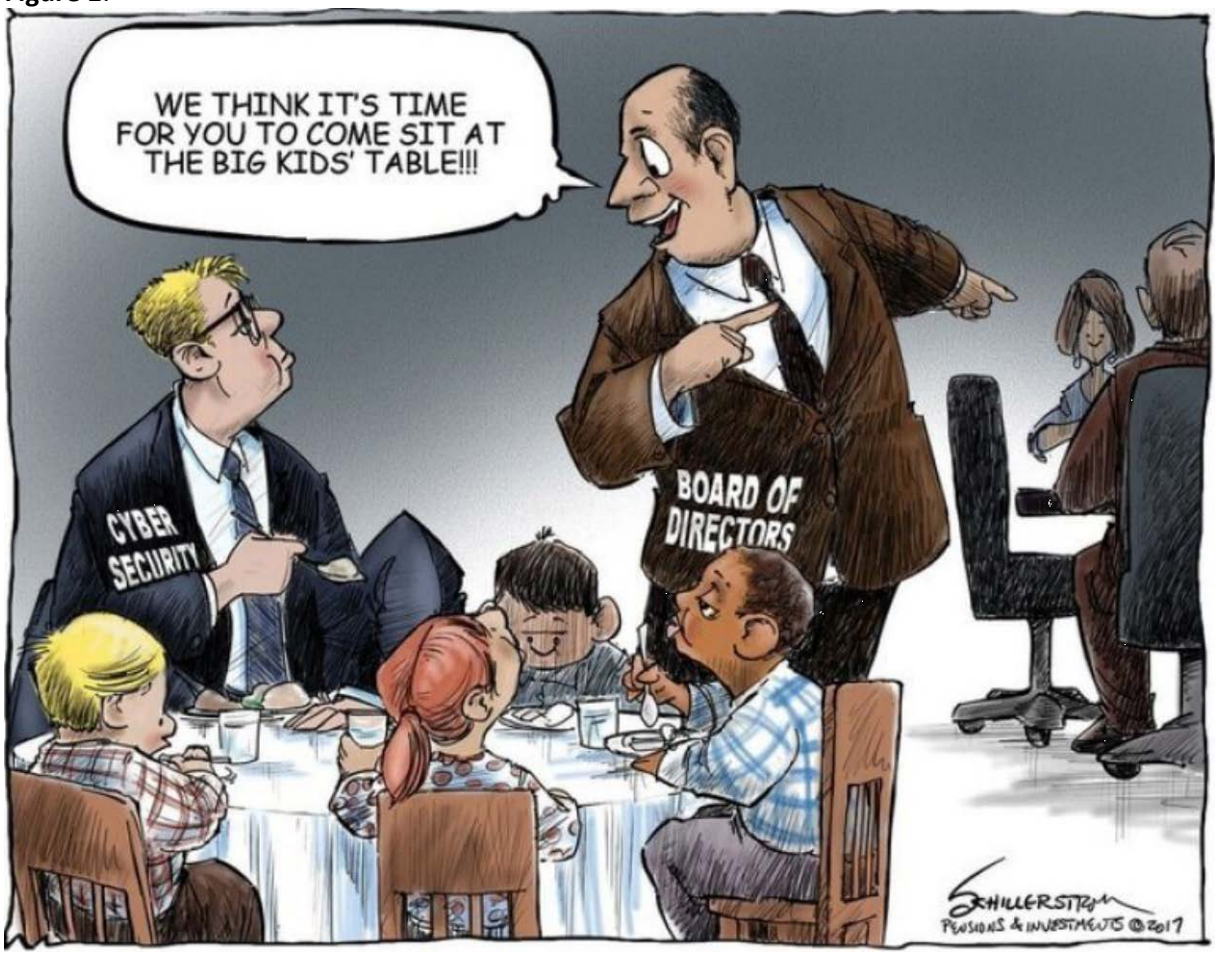
Nicolas Arpagian,
Orange Cyberdefense

Abstract:
Piracy weapons are being commodified like consumer goods as digital technology is more intensely put to use. Once information technology increasingly serves to produce, enhance, store and share data, the risks of cyberattacks increase just as much. By becoming more common, malware of all sorts has effects far beyond the community of computer engineers. Ever more legal experts, investors, financial analysts… are demanding accountancy in matters of protection. Spreading through all layers of private and public organizations, this demand stems from our growing dependency on data and information systems. It is up to consumers and procurement services to choose their providers of technology and digital services by taking into account cybersecurity requirements, which obviously add to costs and come with drawbacks. These technical choices must be based on information about the growing number of legal obligations and about the expenses and processes necessary for evaluating the information produced and deciding who may have access to data and use them. This managerial and strategic overhaul leads us far beyond the simple question of compliance with security rules.

"*We think it's time for you to come sit at the big kids' table*": this punch line used by a cartoonist (Figure 1) refers to the place recently assigned to cybersecurity on boards of directors. Successive reports in the news about cyberattacks against firms and administrations of all sizes, in all sectors and all regions have turned this technical topic into a theme of general interest. Cyberthreats are no longer a topic for computer engineers alone since their effects create serious difficulties or even imperil the use of the digital services that now shape our everyday lives, both personally and professionally. The systematic use of information technology to interact with family, friends, colleagues, partners, customers, suppliers and institutional decision-makers has drawn attention to the need for information system equipment to work normally and for data to be continually accessible. The generalized consumption of digital services, has made cybersecurity an ever more important priority that reaches beyond the technical procedures of computer science.[1]

[1] This article expresses the author's personal opinion and not that of the institutions that he represents. This article has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references. All websites were consulted in February 2020.

Figure 1:

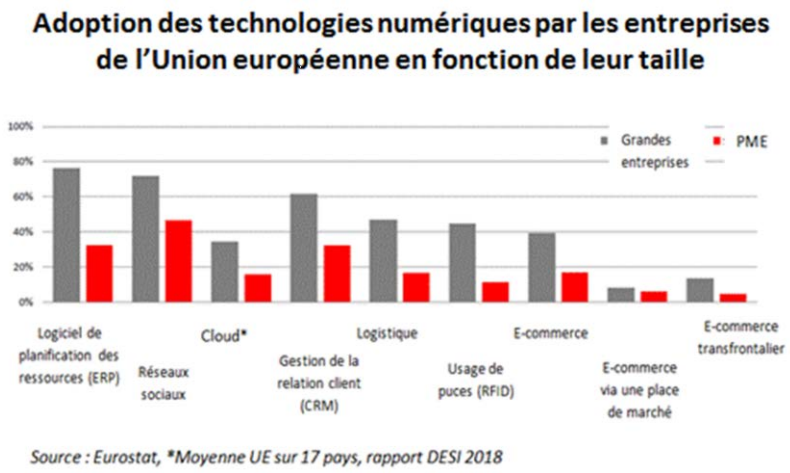


Assuring the availability of means of communication has become a top-ranking preoccupation. If information systems fail, most firms will instantly realize that their activities are paralyzed and that their teams are unable to conduct business normally.

A digital but tangible economy

A quick definition of economics is as the management of scarcity, but it should be brought back under discussion given the switch toward an increasingly dematerialized economy based on the collection, transmission and value of data. Since data are now infinitely duplicable, storable and transferable, consumers/users of digital technology might have the illusion that the data they use day in day out are always accessible.

Figure 2: Adoption of digital technology by firms in the European Union as a function of their size



*Source : Eurostat, *Moyenne UE sur 17 pays, rapport DESI 2018*

Smartphones have become the gateway to banking services, work-related messaging services and social networks (Figure 2). The fluidity of uses and the multitude of services soon convinced the least technophile of cybernauts and mobinauts of the importance of permanent access to these precious devices (GRUNY 2019). The feeling of something missing when users lose or forget their smartphones soon enough introduced them to cybersecurity. Lay persons are interested in digital security as a guarantee of the continuity of services and of access to their store of electronic data. This security must see to the control of computational machinery but while also remaining unnoticed in the background so as not to bother or slow down online browsing.

An expertise diffused but not always shared

The "cyberexpert" has become a character in novels; and fictions on television or in the movies have made ample room for this figure. In the media, the word "hacker" is now a synonym of a "pirate" on the Internet, wrongly so. Hacking should not be prejudged as a form of piracy but instead as the capacity for an autonomy of knowledge so as not to be locked into playing the single role of a passive consumer of technology (ARPAGIAN 2013). It might prove useful for teams who design or sell products to understand how hackers have come to have the upper hand on technology.

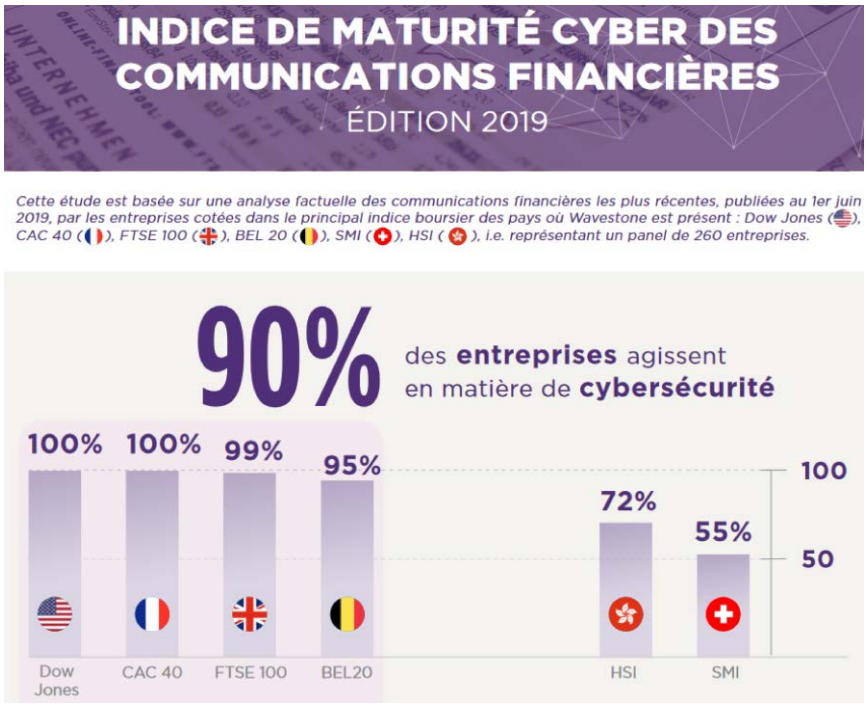
It is not just technical services that should understand the mechanics of information and communication technology (ICT) and its implications. As a consequence of the enforcement of the General Data Protection Regulation in May 2018 in Europe, most firms and public organizations have become aware of the value of data.[2] Give heavy sanctions for the loss or theft of personal data — up to 4% of sales worldwide of the parties held liable — corporate staffs are working with attorneys to make sure that the services that collect, exchange or produce data comply with legal regulations. All stakeholders are cooperating with experts in cybersecurity and ICT for the protection and

[2] GDPR: "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data" available via: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1478961410763&uri=CELEX:32016R0679.

traceability of data and the uses of data in firms. Under the Military Program Act for 2014-2019, France chose to appoint hundreds of operators of vital importance (OIV). Meanwhile, the EU's Network and Information Security (NIS) directive, enforced as of May 2018, has set the protection criteria to be upheld by operators of essential services (OSE).[3] Major sectors of the economy have had to address the question of cybersecurity.

Figure 3: "Cybersecurity maturity in the financial communications of major listed firms", July 2019

Source: Cabinet Wavestone available via https://www.wavestone.com/app/uploads/2019/07/Wavestone-Cybersecurite-Analyse-des-documents-de-references-du-CAC-40-2019_v1.0.pdf.



These legal ultimata with dates of enforcement announced well in advance have stimulated a sharing of know-how between specialists who used to pay no mind to each other. This experience should serve as an example for duplicating or generalizing this multifaceted approach, which is fully in line with ICT's ongoing impact on all branches of the economy. This integration has taken a very concrete form. As an analysis of the publications by the firms listed on major stock exchanges has clearly shown (Figure 3), nearly all of them have reported on their state of cybersecurity and provided concrete evidence of their financial commitments in this field and of their compliance with ever stricter sectoral regulations.

[3] The NIS Directive on the security of network and information systems: Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union available at http://data.europa.eu/eli/dir/2016/1148/oj.

Individualizing uses but with risks

According to an estimate by Gartner, Inc., 30-40% of information technology projects in big organizations are now designed and steered without the involvement of the organization's division of information systems (DIS). This so-called "shadow IT" is available to nonspecialists, who are not engineers in computer science. The teams who work on business processes formulate a need, and software editors provide easily activated solutions that are interoperable with the existing infrastructure and software.

Pushed by ever stronger competition from new players in the economy and the internationalization of markets, managers are forced to continually improve their agility by adapting business processes. The unwieldy machinery of big groups might prove fatal opposite startups. Not necessarily endowed with enough human resources, DISs, many of which lack a genuine spirit for actions at the service of in-house users, have not always proven to be satisfactorily responsive to business teams' changing needs. Service-providers increasingly approach these teams directly with offers to deliver turnkey servers and applications that can be placed in operation immediately. In the enthusiasm for rolling out a long waited-for, innovative solution, security rules and procedures are pushed aside, along with any contradictions between the general conditions for using the material and in-house requirements.

Given this situation, Gartner has predicted that, by 2020, a third of successful cyberattacks against firms will target "shadow IT" resources.[4] The slogan "Business first" forces us to rerank priorities, mainly for the purpose of maintaining positions in sales or winning markets. In this situation, the overall coherence of a firm's information system or scruples about strictly following security procedures might easily be pushed down on the list of priorities. This is the point when the board's commitment to cybersecurity will make a difference, as it balances the advantages of spontaneity, touted by some, with the security approach advocated by others.

Financializing a technical domain

A firm's capacity for remaining agile and thriving is underlaid by the architecture of its information system, a point of potential vulnerability. The information system is a double-faced, single electronic Janus, as experts in financial analytics well know. International financial rating agencies (Standard & Poors and Moodys) have now integrated the metrics of cybersecurity in their simulations for assessing a corporation's value.[5] In the United States, Equifax was the first company, in May 2019, to have its rating lowered as a result of how it managed a massive cyberattack in 2017.[6] Firms have to prove they are capable of appropriating ICT's flexibility but without jeopardizing their own viability or the viability of their ecosystem of partners, subcontractors, wage-earners, customers, etc.

---

[4] Gartner's Top 10 Security Predictions 2016 on https://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/?cm_mmc=social-_-rm-_-gart-_-swg.

[5] Respectively: "S&P Global Ratings360™ to include cyber risk insights from Guidewire software's Cyence Risk Analytics", 16 February 2018 at https://www.guidewire.com/about-us/news-and-events/press-releases/20180216/sp-global-ratings360%E2%84%A2-include-cyber-risk-insights

and FAZZINI K. (2018) "Moody's is going to start building the risk of a business-ending hack into its credit ratings", *CNBC*, 12 November.

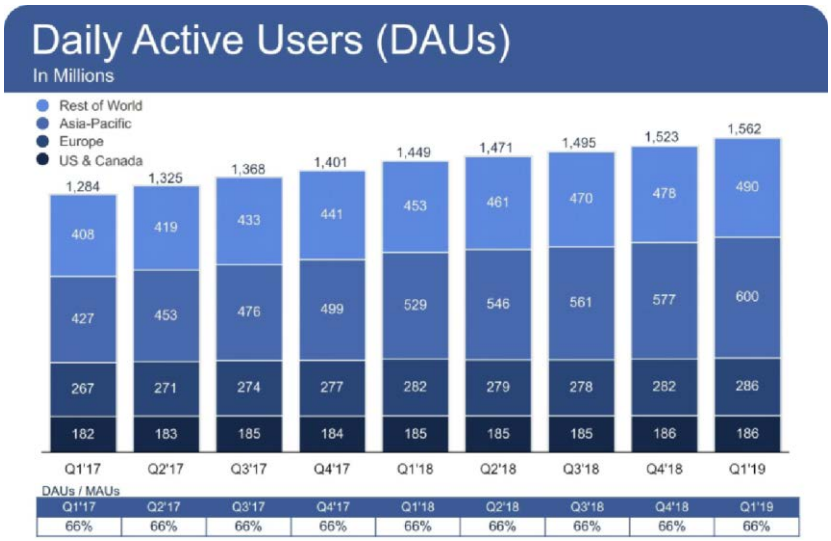
[6] See https://www.moodys.com/credit-ratings/Equifax-Inc-credit-rating-600010933.

Additional requirements are being made through the enforcement of regulations that concern specific branches of the economy. In the United States for instance, the Securities and Exchange Commission (SEC) now sanctions firms that cannot prove they have effectively taken account of cybersecurity regulations.[7] Furthermore, some states want to protect their inhabitants by establishing a strict jurisprudence. New York, for instance, adopted in May 2019 the SHIELD Act (Stop Hacks and Improve Electronic Data Security) to reinforce citizens' rights to data protection.[8] Rules and regulations, with or without carrying sanctions, are for real. All parties, now better informed of ICT-related risks, can, even in everyday matters, chose a service-provider as a function of the confidence they have in the latter's platforms, which will be managing, storing and sharing their data. Ignorance is no longer an argument for not showing interest in digital security.

Is the lack of confidence fatal to firms?

In an information, data-based economy, the question of cybersecurity compels attention since it is an indispensable condition for building confidence between customers and businesses.

Figure 4: Daily active users of Facebook by region.
Source: Facebook.



No doubt about that, in principle… but a notable counterexample is Facebook, a business player so often and seriously blamed for its poor management of users' data. The US Federal Trade Commission (FTC) fined the Californian firm $5 billion in the spring of 2019 for lapses in protecting the confidentiality of its members' personal data. In 2018, the Cambridge Analytica scandal provided proof of how the profiling of Facebook's subscribers could be used for political purposes. In September 2019, the website TechCrunch revealed that Facebook was storing, without precautions

[7] Securities Exchange Act of 1934 – Release N°84429/16 October 2018. Report of Investigation pursuant to Section 21(a) of the Securities Exchange Act of 1934 regarding certain cyber-related frauds perpetrated against public companies and related internal accounting controls requirements, available via https://www.sec.gov/litigation/investreport/34-84429.pdf

[8] New York Senate bill S5575B of 7 May 2019 available via https://www.nysenate.gov/legislation/bills/2019/s6575.

(specifically passwords), the files of 419 million persons around the world — approximately one out of six subscribers. Among these sensitive data were the telephone numbers linked to profiles and, for some accounts, the person's gender and geographical location. Anyone could have access to these data. Despite these serial poor practices, consumers are still enrolling on this social network and participating in its global community. When the FTC announced in the summer of 2019 a record fine for Facebook, Wall Street went bull: the company's stock peaked for the year at nearly $205. All this can probably be set down to consumer dependence on the platform's services, in particular Facebook Connect, which opens access to several interfaces.

Facebook illustrates the compromises that the general public and financial community accept when the services provided are widely appreciated. When ranking priorities, consumers and investors have, in this case, chosen to take a risk.

Conclusion

The increasing digitization of production, sales and communications in all administrative or business activities has made ICT run of the mill, even though it is intimately involved in all our personal and occupational activities. While becoming aware of the dependence on electronic technology and of the value of personal data, information system users are also becoming more demanding with respect to the availability, integrity and confidentiality of their capital of data and of their ICT devices. News reports have drawn attention to the piracy of databases, intrusions with criminal intent on social networks and the lockdown of sensitive information by ransomware. They have thus raised the awareness of cybersecurity in circles extending beyond computer engineers. We hold vendors accountable while access-providers still center their communications around the fact that they do not exploit the data entrusted to them.

The level of education in ICT-related risks is rising. This is the occasion for clients, whether consumers or big firms, to clarify their priorities and choices in relation to this technology. They should prefer solutions for protecting privacy, software that is designed by independent editors or is audited… these decisions must, beyond their technical grounds, take into account legal, political and strategic requirements that do not lie in the hands of ICT experts alone. Will this strong trend among end users substantially influence the policies of big business groups? Were this to happen, other criteria than performance and price would be added onto the list used to select partners, software or equipment. Questions about the finality of uses and the traceability of operations would thus become factors that make or break a deal in this competitive field of business.

Bibliography

ARPAGIAN N. (2009) *L'Avenir de la cybersécurité* (Paris: Institut Diderot).

ARPAGIAN N. (2013) "Les entreprises doivent se mettre au hacking", *Les Échos*, 21 August.

ARPAGIAN N. (2016) "L'Europe de la sécurité numérique: très juridique, mais guère technologique, et encore insuffisamment économique", *Annales des Mines - Réalités Industrielles*, 3, pp.51-54.

ARPAGIAN N. (2017) "Vers une cyberguerre froide entre Moscou, Washington…et la Silicon Valley", *Revue des Deux Mondes*, September, pp. 70-76.

ARPAGIAN N (2018) "Cyberguerre: longtemps annoncée, désormais réalité?", *Rapport RAMSES* (Paris: IFRI-Dunod), pp. 156-161.

ARPAGIAN N. (2018) "Vers une société numérisée, de plus en plus surveillée", *Constructif*, 51, pp.66-69.

ARPAGIAN N. (2018) *Quelles menaces numériques dans un monde hyperconnecté*? (Paris: Institut Diderot).

ARPAGIAN N. (2018) *La Cybersécurité* (Paris: Presses Universitaires de France).

ARPAGIAN N. (2019) "A quoi ressemblera l'*Homo Numericus*?", *Les Échos*, 9 October.

COMMISSION CYBER RISK (2018) *Assurer le risque cyber* (Paris: Club des Juristes) 96p., available via http://www.leclubdesjuristes.com/wp-content/uploads/2018/01/cdj_synthese-du-rapport-assurer-le-risque-cyber_tome-1-de-la-commission-cyber-risk.pdf.

DANESI R. & HARRIBEY L. (2018) "La cybersécurité: un pilier robuste pour l'Europe numérique", Commission des Affaires européennes, Sénat.

ENISA (2019) "Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity".

GRUNY P. (2019) "Accompagnement de la transition numérique des PME. Comment la France peut-elle rattraper son retard?", Report 635 by the Délégation aux entreprises to the French Senate on 4 July.

LACHAUD B. & VALETTA-ARDISSON A. (2018) "La Cyberdéfense", Commission de la Défense nationale et des Forces armées, Assemblée Nationale.

MINISTÈRE DE L'INTÉRIEUR (2019) *L'état de la menace liée au numérique en 2019*, report n°3, May, 142p., available via https://www.interieur.gouv.fr/content/download/117535/942891/file/Rapport-Cybermenaces2019-HD-web-modifi%C3%A9.pdf.

ROUHAN I. (2019) *Les métiers du futur* (Paris: F1RST Editions).

SCHWAB K. (2017) *La Quatrième révolution industrielle* (Paris: Dunod).

SCIENTIFIC ADVICE MECHANISM (2017) "Cybersecurity in the European Digital Single Market", European Commission.