IBIMA Publishing
Journal of Information Assurance & Cyber security
https://ibimapublishing.com/articles/JIACS/2021/630400/
Vol. 2021 (2021), Article ID 630400, 8 pages, ISSN: 2165-9923
DOI: 10.5171/2021.630400

Research Article

Cybersecurity, A Priority of The Modern World

Dan-Alex Ceaușescu-Constantinescu, Andreea-Alexandra Chiriac (Roșca) And Claudiu Chiriac

University of Economic Studies, Bucharest, Romania

Correspondence should be addressed to: Claudiu Chiriac; chiriacclaudiu14@stud.ase.ro

Received date:24 August 2020; Accepted date:26 August 2021; Published date: 1st November 2021

Academic Editor: Bogdan Ghilic-Micu

Abstract

Data is probably the most valuable resource of our time, similar to what represented oil a century ago. Technology giants built their competitive advantage on the huge amount of data they are dealing with to drive the biggest societal changes. The disputes on data created the premises for a new industry to emerge – cybercrime. Cybercrime became a threat not only for the processes of the organizations but also for individuals as unethical data use can change people's attitudes and behavior not only towards the products and services, they are buying but also their political views and values. The purpose of this paper is to assess the dimensions of data security, ethics, and compliance in the context of new regulations.

Keywords: Technology, People Behavior, Data Security, Data Compliance, Regulation

Introduction

There are 2.5 quintillion bytes of data produces by us every day especially generated by internet, social media, communications, digital photos, services and the internet of things [1]. Impressive statistics regarding the main sources of data:

- More than 4.5 billion people use the internet [2], so about 60% of the entire population.
- On average, there are more than 40,000 searches on Google every second, so more than 3.5 billion searches every day [2].
- More than a third of the world's population is active on Facebook monthly [2].
- Every minute on Facebook there is 510,000 comments posted, 293,000 statuses updated, and 136,000 photos uploaded [3].
- Every minute we send 16 million text messages [2].

Cite this Article as: Dan-Alex Ceaușescu-Constantinescu, Andreea-Alexandra Chiriac (Roșca) And Claudiu Chiriac (2021), " Cybersecurity, A Priority of The Modern World", Journal of Information Assurance & Cyber security, Vol. 2021 (2021), Article ID 630400, DOI: 10.5171/2021.630400

- In 2017, there were 4.7 trillion photos stored [2].
- Every minute there is more than 45,788 uber trips [2].
- There will be more than 20.4 billion connected things by 2020 according to Gartner [4].

Moreover, the systematic progress makes the technology even more affordable even free when it comes to services such as GPS, camera, news, banking all being integrated today in our mobile phone without any cost associated. Freemium, the combination of "free" and "premium" is a new business model especially for app developers who design the app adding premium features but make it free so as to attract a considerable user base while the source of revenue is coming from in-app advertisement or from a small portion of users which is paying for some additional features [5].

On the other hand, all this data reveal precious information about us from our usage behavior to what are our preferences, interest, opinions, and hobbies. These insights are the fuel for the brands and organizations to make data-driven decisions to design customized products or services according to our needs and interest. Personalized products or services are becoming a significant part of our life because of their applicability and usability in different areas, allowing us to monitor our health and personal finance, shop online, play games, listening to the favorite songs and taking online courses to grow the skills we are interested in. But this is the mechanism of generating more and more data about us, data that makes the algorithm proficient in predicting our preferences and expose us to advertising that fits our desires and lifestyle.

At the same time, companies are looking for new ways of making sense of the huge amount of data to enhance the current products and services, to innovate in new areas, but also to optimize and automatize the business processes. This is why a new set of tools to analyze structured and unstructured data had been developed recently and there are some new skills in demand on the human resources market. Data guru, so the person who knows how to extract data, analyze it and look for patterns - skills that can improve the use of resources, value chains, managerial operations, industry knowledge, and growth opportunities, is a type of employee the companies are looking for [6]. Moreover, data scientist is one of the most promising jobs in 2019 [7].

According to McKinsey, data, and analytics not only changed the business practice, but data monetization is becoming another source of revenue by adding new services to current offerings, developing new business models, joining with similar companies to create a pool of related data that can benefit all of them [8].

Knowing what the main sources of data are, how this data are generated and the technological premises, it is quite easy to imagine that the process of producing, analyzing and integrating data in the main sources that generate them is intensifying continuously its peace.

Technological trends impact data collection and processing

Technology is rapidly shaping the way companies work and how we interact with the world. Specialists encourage closely looking over five new areas: Artificial Intelligence, Augmented Reality, Blockchain, Automation and Internet of things [9].

Artificial Intelligence (AI) is a computer area which has as the main purpose to mimic how people acquire the necessary knowledge, resonate, solve problems, perceive, learn, plan, manipulate and move objects. Machines can act and react as humans only if they have enough information to be used by its algorithms to identify patterns [10].

Augmented Reality (AR) is the technology that overlaps the virtual objects in the existing environment, as a result, the information addon creates a new artificial reality. Many augmented reality apps have been developed recently to enhance different industries from gaming to constructions, this technology having the

potential to influence even more our lives [11].

Blockchain is a huge distributed database that runs on millions of computers and it is open source, so anyone can access the code to see what any structured information from banking transactions to information about who married whom or who owns what land or what light bought power from what power source. This is a way of proving the truth through mass collaboration establishing a source of trust in a world of distrust [12].

Automation is the process that increases efficiency and reliability by replacing manual operations or increase the speed for repetitive tasks. The potential of automation is huge, its impact in manufacturing is already known by decreasing the workforce in this industry but now it moves to more sophisticated jobs replacing the car drivers, pilots, public-sector jobs or teachers [13].

Internet of Things (IoT) is the concept of connecting any device through the internet such as smartphones, coffee makers, washing machines, lamps, wearables or any other objects including components of different machines. The purpose of having all these objects inter-connected is to make life much easier, for example, if the alarm clock is set for a specific hour, it can be linked with the coffee maker to have coffee prepared in the morning [14].
These trends are connecting with the data generation or processing. While IoT is the main source of data and AR is bringing data from a different reality, AI and automation bring new opportunities to process data and drive actionable insights and Blockchain collects data in an immense database.

Technology came with many risks associated to data

The expansion of data volume has many risks associated as the data protection regulations and the set of tools that ensure security doesn't keep the same pace with what we produce every day. Risks include applications, users or devices.

There are a few famous examples of data breaches. Cambridge Analytica is a name that resonates with the USA elections and the Brexit campaign because of its involvement as a data analytics firm that accessed 87 M of Facebook profile to build an algorithm that was able to predict an influence vote choice. This was the biggest data breach that involved the tech giant. Everything started with a group of thousands of Facebook users that were incentivized to take a personality test and agreed to have their information collected for an academic purpose. Not only their personal information was collected, but also their Facebook friends which allowed the algorithm to learn from more data and to improve the prediction accuracy and microtargeting with the customized campaign messages. Facebook denies that the harvesting of the Facebook profiles was a data breach as Cambridge Analytica and the companies they worked with got access to the information legitimately, the only rule breaker was the fact that the information was used for third parties. Cambridge Analytica, Facebook, and the other companies are investigating by the British Information Commissioner's Office for the Brexit campaign, by the Electoral Commission for the role played in the EU referendum and by many US institutions from House Intelligence Committee to FBI. The only price paid by Facebook so far was the drop in its share value [15].

There are other examples of the sensitive data that has been exposed over the last years [16]:

- About 15 Bn. of data records have been lost or stolen since 2013.
- Only 4% of breaches were secure, the data were encrypted to be useless
- 86% of the incidents occurred in North America.
- There are 6.5 M of data compromised every day, so 75 records compromised per second.
- 42% of data breaches are caused by hackers or criminals while 29% are caused by system glitches.
- ¼ of the incidents is caused by the employees.

- In the US the main data breaches were in Business (45.9%) and Medical (29.2%) sectors.
- Top 3 data breaches from the last 15 years were generated by American Online in 2013 impacted 92 M screen names and email addresses, Yahoo in 2013-2014 compromised all 3 Bn. accounts and Target in 2013 impacted 110 million accounts [16].

With the new technological advancements, there are many ways to use the technology to process apparently inoffensive personal data to create algorithms that are able to manipulate every choice we make not only regarding the brands we buy or use but also regarding the political options or the general opinions and values. Hacking humans is the ultimate risk for our data as a deeper understanding of the human decision-making process; the algorithms become more reliable at these types of tasks, at the same time making us less reliable. After the human operating system is hacked, a precise kind of manipulation, advertisement and propaganda will follow [17].

For 2020 companies there are ten risks when it comes to data privacy [18]:

- **Accidental sharing**, so the company's employees share sensitive information with someone outside the organization.
- **Overworked cybersecurity teams**, as the incidents number increases, and the security specialists are quite rare.
- **Employee data theft** means the insider threat which is coming mainly from employees who are not in leadership positions.
- **Ransomware attacks** that are designed to block a computer system until a sum of money is paid are on the rise, in 2019 the cost of a ransomware attack more than doubled.
- **Bad password hygiene** as some of the login credentials are already compromised by previous data breaches or other employees that have redundant or easy to guess passwords.
- **Bribery** of the employees to expose the company's data or to plant malware on the network.
- **Too much data access** as data is one of the main resources of the company, each employee should access only what he or she needs to know for that position.
- **Phishing emails** are on the rise and the technology makes the attack even more sophisticated.
- **Fraud** by taking the email addresses and passwords that enable even more elaborate attacks.
- **Denial** of the companies to understand the risks associated with the data to be equipped and train the employees to avoid the risks [18].

The biggest challenge of the companies is the sense of losing control over data that comes with utilizing third-party solutions for cloud, data management and analytics [19]. Moreover, according to a survey of 250 C-level leaders in the UK, data breaches and hacking attacks is the new reality for the companies [20].

Data security and cybersecurity

In this context with many risks associated with data, there is a focus on big data security market which is expected to register a CAGR of 17% between 2019 to 2024, concerns associated with data exposure being both for on-prem and on cloud systems [21]. New threats related to data privacy emerge and it is impossible to invest in eliminating them, but there are some preventive practices to help companies protect their data and their clients' data such as [22]:

- **Strong security policies and practices** and here everything starts with the efficiency of the data collection to have the optimal amount of data that can be manageable, but also the strategy for the incident response and backup recovery and the

employees' familiarity with the procedures.
- **Access control** is related to giving the employees access only to the part of the network necessary for their activity.
- **Network Protection** through antiviruses, firewalls, and proper maintenance.
- **Encryption** which assures the data privacy even if the data is stolen because encrypting, it becomes useless [22].

Going even further, Gartner identified top security trends for this year and beyond that should be monitor over time to see the traction they get [23]:

- **Risk Appetite Statements Are Becoming Linked to Business Outcome**: IT strategies are aligned to business goals, security and risk management is gaining importance in the business decision.
- **Security Operations Centers (SOCs) Are Being Implemented With a Focus on Threat Detection and Response**: the focus in security shifts from prevention to detection and this involve building SOCs that will be able to integrate threat intelligence, consolidate alerts and automate response.
- **Data Security Governance Frameworks (DSGF) Will Prioritize Data Security Investments**: DSGF identifies data and defines data classifiers and data security policies, information that can be used to select technologies that minimize the risk.
- **Passwordless Authentication Is Achieving Market Traction**: authentification through Touch ID OR face recognition is becoming more popular and it increases both usability and security.
- **Security Product Vendors Are Increasingly Offering Premium Skills and Training Services**: Vendors' security services range from partial to full support to complement the unfulfilled cybersecurity roles.
- **Investments Being Made in Cloud Security Competencies as a Mainstream Computing Platform:** the shift to the cloud brings even more discussions related to security as it is the cloud customers' responsibility to keep it secure [23].

Data security is a growing area that fulfills the growing need of protecting the huge amount of data. Still, there is still a need of changing the paradigm to prevent the data breaches by simplifying the business processes, but also of developing easy to use security solutions that are abe to quick response to attacks and the stringent need of covering the skills gap on data security.

Data protection through regulations

Data protection and ethical use of personal information is not only the company's responsibility, but it is also necessary to have a uniform standard applied by the governments or other types of institutions to protect citizens' personal data. Recently European Union came with regulations on both general data protection and also on artificial intelligence, the technology that uses a big volume of data to learn and develop dynamic algorithms based on the input data to take accurate decisions in different fields.

General Data Protection Regulation (GDPR) came into effect starting with May 2018, it applies only to the EU and it affects every company that stores and processes customer data from tech companies to marketers and research agencies that connect them. The directive is giving the individuals more power over less data, at the same time the companies that collect data and use it for the monetary purposes have less power. GDPR is giving to individuals 8 basic rights: to access their data; to be forgotten, in the case they are not clients anymore or withdraw their consent; data portability, so the right to transfer their data from one provider to another; to be informed before data is gathered so the consent is necessary not implied; to have the information corrected; to restrict the processing; to object, to stop processing for

direct marketing; to be notified in 72 hours in case of data breaches [24].

Moreover, the tech companies updated their politics to comply with GDPR, for example, Facebook created privacy options to put the users in control over their information to find and delete specific information on the site. Apple revealed its privacy dashboard while Google quietly updating its products and privacy policies [25].

On April 2019 European Commission's published the Ethics Guidelines for Trustworthy Artificial Intelligence (AI) designed by a set of experts and followed by a piloting program to collect feedback on how the guidelines should be implemented. The guidance sets key requirements to achieve Trustworthy AI: human agency and oversights; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination, and fairness; societal and environmental wellbeing; accountability [26].

US lawmakers have introduced a bill – the Algorithmic Accountability Act planned for the companies with a large volume of data to assess the algorithms behind the automated systems to be sure these are not discriminatory or pose privacy or security risk [27].

Acknowledgement

This paper was co-financed from the Human Capital Operational Program 2014-2020, project number POCU / 380/6/13/125245 no. 36482 / 23.05.2019 "Excellence in interdisciplinary PhD and post-PhD research, career alternatives through entrepreneurial initiative (EXCIA)", coordinator The Bucharest University of Economic Studies."

Conclusion

Data is one of the most valuable resources of this century but, at the same time, it can make us as individuals extremely vulnerable to manipulation, propaganda or impact the business processes or resources of the companies. Data can be an easy target as it can be compromised in different stages of the process from data collection to storage and analysis. On the other hand, the cyberattacks are becoming more sophisticated with the technology progress; this is why the security industry is developing new tools and skills and the authorities design regulations to better protect data.

References

- Marr, B., 2018a. *How much data do we create every day? The mind-blowing stats everyone should read.* [Online] Available at: https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#632327c860ba [Accessed 20 August 2019].
- Internet World Stats, 2019. *Internet users distribution in the world - mid-year 2019.* [Online] Available at: https://www.internetworldstats.com/stats.htm[Accessed 20 August 2019].
- Noyes, D., 2019. *The top 20 valuable Facebook statistics – updated September 2019.* [Online] Available at:https://zephoria.com/top-15-valuable-facebook-statistics/ [Accessed 20 August 2019].
- Marr, B., 2018a. *How much data do we create every day? The mind-blowing stats everyone should read.* [Online] Available at: https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#632327c860ba [Accessed 20 August 2019].
- Kumar, V., 2014. *Making "Freemium" work.* [Online] Available at: https://hbr.org/2014/05/making-freemium-work [Accessed 20 August 2019].
- UTS University, 2019a. *Five tech trends for 2019.* [Online] Available at: https://www.uts.edu.au/about/faculty-engineering-and-information-technology/postgraduate/articles/five-tech-trends-2019 [Accessed 20 August 2019].

- Rayome, A. D., 2019. *Why data scientist is the most promising job of 2019.* [Online] Available at: https://www.techrepublic.com/article/why-data-scientist-is-the-most-promising-job-of-2019/ [Accessed 20 August 2019].
- Gottlieb, J., 2017. *Fueling growth through data monetization.* [Online] Available at: https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/fueling-growth-through-data-monetization [Accessed 20 August 2019].
- UTS University, 2019b. *Top skills employers are looking for.* [Online] Available at: https://www.uts.edu.au/about/faculty-engineering-and-information-technology/postgraduate/articles/top-skills-employers-are [Accessed 20 August 2019].
- Technopedia, 2019. *Artificial Intelligence (AI).* [Online] Available at: https://www.techopedia.com/definition/190/artificial-intelligence-ai [Accessed 25 August 2019].
- Marr, B., 2018b. *9 Powerful real-world applications of Augmented Reality (AR) today.* [Online] Available at: https://www.forbes.com/sites/bernardmarr/2018/07/30/9-powerful-real-world-applications-of-augmented-reality-ar-today/ [Accessed 25 August 2019].
- Tapscott, D., 2016. *How blockchains could change the world.* [Online] Available at: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/how-blockchains-could-change-the-world [Accessed 25 August 2019].
- Market Business News, n.d. *Automation,* s.l.: Market Business News.
- Morgan, J., 2014. *A simple explanation of 'The internet of things'.* [Online] Available at: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#393ab19b1d09 [Accessed 25 August 2019].
- Graham-Harrison, C. C. a. E., 2018. *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach.* [Online] Available at: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election [Accessed 25 August 2019].
- Desjardins, J., 2019. *The 15 biggest data breaches in the last 15 years.* [Online] Available at: https://www.visualcapitalist.com/the-15-biggest-data-breaches-in-the-last-15-years/ [Accessed 25 August 2019].
- Harari, Y. N., 2018. *21 Lessons for the 21st century.* s.l.:Spiegel & Grau, Jonathan Cape
- Kohen, I., 2019. *10 Data security risks that could impact your company in 2020.* [Online] Available at: https://www.forbes.com/sites/theyec/2019/10/01/10-data-security-risks-that-could-impact-your-company-in-2020/ [Accessed 1 October 2019].
- Digital Guardian, n.d. *Data security knowledge base.* [Online] Available at: https://digitalguardian.com/dskb/big-data-security [Accessed 12 September 2019].
- Kobie, N., 2019. *Carbon black: attacks and breaches the "new normal" for businesses.* [Online] Available at:https://www.itpro.co.uk/cyber-attacks/34545/carbon-black-attacks-and-breaches-the-new-normal-for-businesses [Accessed 1 October 2019].
- Mordor Intelligence, n.d. *Big data security market - growth, trends, and forecast (2019 - 2024).* [Online] Available at: https://www.mordorintelligence.com/industry-reports/big-data-security-market [Accessed 3 September 2020].
- Weicher, J., 2019. *Best practices for data security.* [Online] Available at: https://www.itprotoday.com/business-resources/best-practices-data-security [Accessed 1 October 2019].
- Costello, K., 2019. *Gartner identifies the top seven security and risk management trends for 2019.* [Online] Available at: https://www.gartner.com/en/newsro

om/press-releases/2019-03-05-gartner-identifies-the-top-seven-security-and-risk-ma [Accessed 12 September 2019].

- Lund, J., 2019. *What is GDPR and how does it impact your business?.* [Online] Available at: https://www.superoffice.com/blog/gdpr/ [Accessed 12 September 2019].
- Hern, A., 2018. *What is GDPR and how will it affect you?.* [Online] Available at: https://www.theguardian.com/technology/2018/may/21/what-is-gdpr-and-how-will-it-affect-you [Accessed 12 September 2019].
- Lisa Peets, M. H. S. J. C. a. G. N., 2019. *EU high-level working group publishes ethics guidelines for trustworthy AI.* [Online] Available at: https://www.insideprivacy.com/artificial-intelligence/eu-high-level-working-group-publishes-ethics-guidelines-for-trustworthy-ai/ [Accessed 12 September 2019].
- Robertson, A., 2019. *A new bill would force companies to check their algorithms for bias.* [Online] Available at: https://www.theverge.com/2019/4/10/18304960/congress-algorithmic-accountability-act-wyden-clarke-booker-bill-introduced-house-senate [Accessed 12 September 2020].