Data Protection, Laws and Cybersecurity

Krishna Annugula
Information Technology, Master's Program
Metropolia University of Applied Sciences
Espoo, Finland
Krishna.Annugula@metropolia.fi

***Abstract*— This paper explores about data, data protection, laws, data breaches, cybersecurity, cyber-attacks, regulatory compliance, and advice. In the recent days usage of the internet has increased rapidly, along with that a lot of cybersecurity incidents and data breaches also increased. Keeping in mind about increased incidents the paper explains why data protection and cybersecurity should combine.**

Keywords: Data; Data security; Data brokers; Data protection laws; Data breaches; Cybersecurity; Cyber-attacks; Regulatory Compliance; Advice; Risk; Analysis.

I. INTRODUCTION

In today's digital era, data plays an enormous role in our daily lives. Nowadays, nothing happens without the use of information technology or the Internet, considering on-line purchases, remote-education, videos, audios, etc. Where it was involved in all types of age groups. Especially this pandemic situation has led to an inevitable surge in the use of digital technologies over pre-pandemic. As part of this we as humans provide the personal data to access the websites or accept the cookies, as we don't know or we never thought that what kind of data has been collected because data collection is less visible for us. One of the surveys stated that the data was collected and that they created a profile and sold it for advertising. A profile may add up to 1,500 points. There are many false and malicious web sites collecting a lot of data. To access the website, of course, we must submit personal information, otherwise we cannot use the website.

If we are not aware of which type of website was searched or clicked on the pop advertising links. If the link targets a malicious website, then our computer is threatened by cyber-attack, or the personal data provided have been misused by cyber criminals, then we are under surveillance of cyber-attack and may become a victim of it.

As a result, with the increased use of information technology, data security and cybersecurity have become crucial elements of human life.

Data protection and cybersecurity are interdependent. If the data is secure and in good hands, then we have a much lower chance, if not a negligible percentage, of falling under cyber-attacks.

II. DATA PROTECION, LAWS AND CYBERSECURITY

A. *Data Protection*

First, we need to be aware of what data is and why it needs to be protected.

Simply put, the data means, The key pieces of information that businesses typically store, whether it's employee records, customer information, health records, loyalty schemes, financial transactions [1].

As per Fig.1, these are the types of data viewed on computers that are Geographic, Transport, Natural, Cultural, Scientific, Financial, Statistical and Meteorological [2].

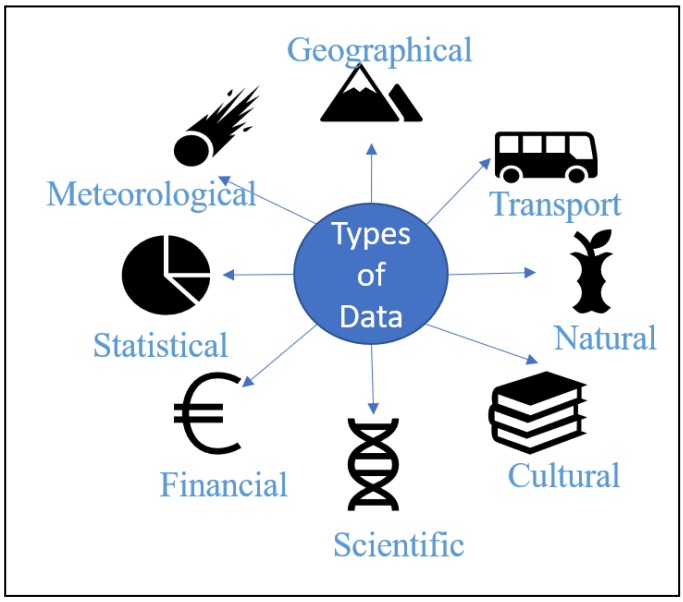

Figure 1. Various types of data vizualized on comptuer

1. *How Data is collected*

Data is collected in different ways such as over the emails, phones, by the interviews, lucky draw coupons, loyalty schemes, survey questioner, health records, etc. The common type of data stored by data brokers are Name, Emails, Contact details, Banking information, Credit information, Health information, IP address, Vehicle registration number etc.

2. *Data protection & laws*

The importance of data protection increases with the increase in the number of data created and stored. Data must be protected to prevent misuse of data by third parties for scams, such as identity theft and phishing.

Yes, of course, data protection requires a law, The first Data Act was introduced in Sweden in 1973 and called as Sweden's Data Act 1973.This the first comprehensive national data privacy law [3].

Every country has its own data protection laws. "Over 89 countries and independent territories, including nearly every country in Europe and many in Latin America and the Caribbean, Asia, and Africa, have now adopted comprehensive data protection laws." [3]

The Data Protection Act (DPA) was adopted by the United Kingdom government in 1998. "The Data Protection Act 1998 was the law governing the processing of personal data by all organizations, be they public or private, including charities. All data breaches in the UK are investigated by the Information Commissioner's Office (ICO) and the same was true then, although the act provided guidelines for the type of penalty that could be applied if someone was found to have been in contravention of the rules" [4]. If someone does not comply with the DPA, the consequences can be serious, with fines of up to £500,000 or imprisonment.

"The European Union has the General Data Protection Regulation (GDPR). The GDPR was adopted on 14 April 2016 and became enforceable beginning 25 May 2018." [5]

B. Cybersecurity

First, we need to learn a little more about cybersecurity by determining what cybersecurity is and why it needs to be secure.

The term cybersecurity is disputed. Its definition can vary even from one government department to another. There are over 400 cyber-related definitions. This is illustrated by the New America foundation study in 2014.

Simply put, "Cybersecurity is about protecting Internet-connected systems, including hardware, software, and data, against cyber-attacks. It has two words; one is cyber and other is security. Cyber relates to technology that contains systems, networks, programs, or data. Whereas security associated with protection includes system security, network security, and application and information security." [6]

1. *Importance of cybersecurity*

October is a national cybersecurity month, an annual awareness campaign on the importance of cybersecurity. Cybersecurity is important, regardless of the size of the organization.

Below are few points, which tells about the importance of Cybersecurity.

Cybercrime is on high rise: There are approximately 4,000 cyber-attacks every day. The reason behind the rise of cybercrimes is that it is less expensive, faster and more cost-effective compared to other types of crimes. It is impossible to find or access the locations of the criminals, as they use the Darknet for this attack and in return, they only accept cryptocurrency as bitcoins for financial transactions.

Damage is extensive: Cybercrime can cost the organization millions of euros in loss, It is not only the financial cause, but also harm the reputation of the organization, ability to do business, compromise the physical security and health of employees, customer relations and a lot more.

Cybersecurity builds trust: Cybersecurity flaws impacts the trust of clients and employees. If people don't feel their information is protected, then clients and employees don't have confidence in the brand, the product, and the services.

Protect our identities: In the digital age, the user's identity protects billions of data points, which are shared by IOT devices or personal information over networks. Securing these identities will reduce the risk of cybercrime for the organization and individuals.

Every organization has vulnerabilities: When organizations fall, merge, and develop over time, their networks and systems naturally become more complicated and things muddle up to the cracks. In addition, end-users can be the weakest wing in an organization's security, which requires the organization to deploy robust, secure and compliance protection in place.

We should all be concerned about cybersecurity, which is part of our job, because it's a critical part of every organization. A well-implemented security approach can help us maintain a strong and secure private workplace.

2. *Cybersecurity categories*

Cybersecurity may be broken down into few general categories, as show in Fig. 2 [7]

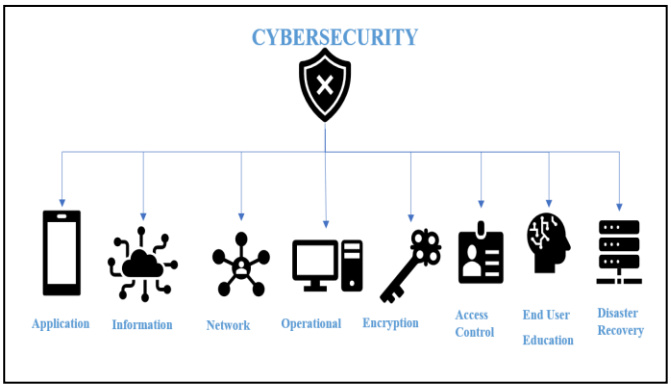

Figure 2. Few general catgeories of Cybersecurity

- **Application security**: Focus on maintaining security for software and devices, free from threats.
- **Information security:** to protect and secure the privacy and integrity of data at rest or in motion. It is also known as Data protection.
- **Network security**: Securing a computer network against malicious actors or unauthorized access

that may constitute a targeted attack or malicious program.

- **Operational security**: Create and maintain processes, procedures, and decision-making for processing and safeguarding data assets.
- **Encryption:** A method of transforming the message or information into an unreadable format for non-authorized users using a special algorithm.
- **Access control**: Establish rules and policies to limit access to physical resources or a system or virtual resources.
- **Safety awareness training**: Address the education of people who often create security vulnerabilities because of their actions or lack of knowledge. People may unintentionally introduce a virus or malware into a security system if they are not familiar with the best security practices, such as deleting suspicious attachments in emails, forbidding the insertion of unidentified USB keys, etc.
- **Business continuity and disaster recovery**: Determine how an organization responds to a cybersecurity incident or data breach. Policies and procedures dictate how the organization regains control over its operations.

III. DATA BREACHES AND CYBER ATTACKS

A. Major incidents on data breaches and Analysis

Simply put, data breach is a security incident, in which information is stolen from a system without authorization or knowledge of an owner's computer network or email accounts. Another way of data breach is to sell personal data by data brokers to advertising companies and personal data is misused by cybercriminals.

According to the **PR Newswire** publication, New York, 15 Oct 2020. below is the analysis.

"The research covered 50 medium-sized personal data breach cases with a damage scale of more than 1,000 cases and less than 1 million cases caused by unauthorized access and uploading the photos into social media. The cases of data breaches were classified into eight sectors:
manufacturers, retail trade, services and infrastructures, software and telecommunications, commercial companies, financial services, advertising/publishing/media, and government/public offices/organizations, based on the information of the companies that announced the breach." [8]

Retailers were the most exposed to data breaches, with 24%, followed by services and infrastructure, with 22% and manufacturers, with 18%. On the other hand, only 6% of breaches occurred in the financial sector. This is ratio of Public Companies (including subsidiaries) and Private Companies in Data Breach incidents.

Let us see how these data breaches took place. According to the Data Breach Investigations Report (DBIR) by Verizon. Below Fig.3 shows Statistics of Common features of data breaches. [9]

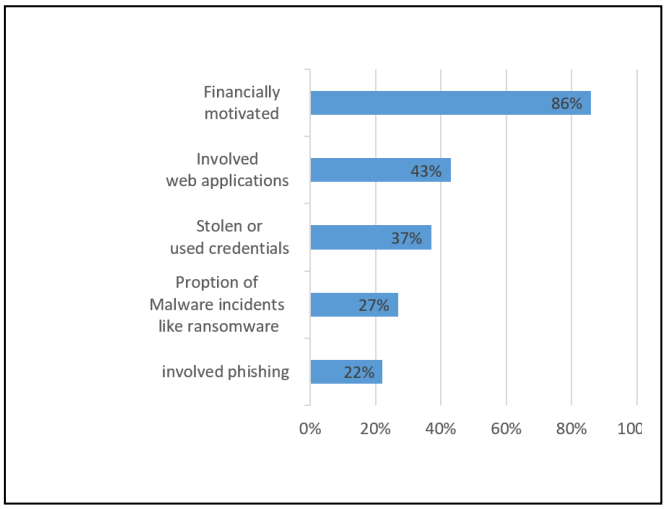

Figure 3. Statistics of Common features of data breaches

Let's look at the most significant breaches in cyberspace. According to author Dan Swinhoe, there are 15 largest data breaches of the 21st century [10]. I took 5 the largest and greatest number of data breaches of the authors point.

- Adobe
  This occurred in October 2013 with an impact on 153 million user files.
- Adult Friend Finder
  This occurred in October 2016 with an impact on 412.2 million accounts.
- Canva
  This occurred in May 2019 with an impact on 137 million user accounts.
- eBay
  This occurred in May 2014 with an impact on 145 million users.
- Equifax
  This occurred on July 29, 2017 with an impact on 147.9 million consumers.

Vastaamo (Finnish psychotherapy center) has been one of the biggest criminal investigations in Finland based on the number of victims its about 40,000 person data. Hackers demanded around 450,000 euros in exchange during October 2020. [11]

B. Cyber-attacks, How attacks are Performed?

Simply put, an attack via cyberspace, targeting one or more computers or networks with the aim of destroying, deactivating, disrupting or maliciously controlling an IT environment or infrastructure. A cyber-attack may also be defined as the theft of controlled information or the destruction of data integrity.

All attacks have the potential to target people, processes, and technologies. Let's look at the latest statistics on cyber-attacks in 2020.

There are 9 key cybersecurity statistics briefly, as shown in below list. [12] .

- $17,700 is wasted every minute on phishing attacks.
- 94% of malicious software is delivered through email.
- 40% of IT leaders report that cybersecurity positions are the most challenging to fill.
- 60% of the breaches were related to vulnerabilities where a fix was available but not implemented.
- Phishing attacks make up over 80% of reported security incidents.
- 63% of businesses said their data was potentially compromised in the past 12 months due to a hardware or silicon security vulnerability.
- Attacks against IoT devices tripled in H1 2019.
- Data breaches average $3.92 million for companies.
- File-less attacks increased 256% in H1 2019.

Let's have a deep understanding of how attacks are performed. As the presenter "Tommi Vihermaa" said during the session on ICT trends, the explanation of cyber-attacks is done in stages as shown in Fig.4 [13]. If the target seems too difficult to achieve, attackers will select an easier target.

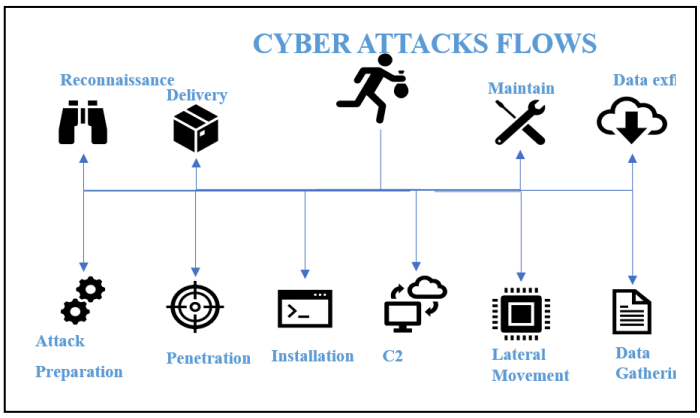

Figure 4. Cyber-attacks are performed in phases.

- **Reconnaissance** (Information gathering): search, passive or active, target identification and target selection.
- **Attack preparation** (Weaponization): Generate payloads, prepare exploits such as execution code, AV escape, bundle with the delivery file.
- **Delivery**: Transmission of the payload (malware) to the target through email, websites, USB drives, other file delivery mechanisms, third-party compromise website, inject malicious code.
- **Penetration** (Exploitation): Exploiting vulnerable systems likes Usually recently published vulnerabilities, Unpatched systems, Zero-day exploits, Configuration weaknesses, Remote Access Trojan (RAT).
- **Installation** (Persistence): Establish persistence as programmed tasks and services, manipulate the Windows registry - autorun, escalate privileges, exploit the local machine to gain high privileges, harvest identifiers, passwords, service accounts.
- **Command & Control** (C2): Keeping the control channel to the target from the outside as Maintain access to the target environment, Control channel often masked as legitimate network traffic, DNS requests, Http and HTTPS traffic, Attacker infrastructure often in Azure, AW and other cloud provider.
- **Post exploitation phase** (Actions on objective): Move Laterally, Steal Data, Data Collection, Cyber Spying, Make Money, Ransomware, Crypto jacking, World Data Markets.

IV. Regulatory Compliance And Advice

To overcome these data violations and cyber-attacks, every individual and every organization must follow certain rules.

A. Regulatory Compliance

Here is a measure of regulatory compliance for corporate safety.

- Policies Managements.
- Security Regulations.
- Rules.
- Standards.
- Adhering to Law.

B. Data protection guidance

Key guidance on data protection to ensure information security.

- Use strong encryption.
- Prioritize staff training.
- Minimize data use.
- Store data no longer than necessary.
- Ensure crisis resilience.
- Manage passwords properly.
- Invest in a visitor management solution.

C. Cybersecurity advice

Organizations should take some critical safety advice.

- Assess current security status.
- Continuously maintain and improve security posture.
- Keep an eye on information security incidents.
- Prepare by practicing.
- Maintain security expertise.

V. CONCULSION

A. Combine Data Protection And Cybersecurity

The article “Why Data Protection and Cybersecurity Can't Be a Separate Functions?”, is published on YEC COUNCIL POST by Dmitry Dontov, CEO and founder of Spin Technology, a cloud-based data protection company based in Palo Alto” [14]. As per his view data protection and cybersecurity are linked to each other and it should be combined. Below is the good explanation.

“Why Combine Cybersecurity and Data Protection?

A recent hack affected the U.S. Department of Veterans Affairs and put the personal information of approximately 46,000 veterans at risk. Cybercriminals tried to divert payments from the department by using social engineering techniques and exploiting authentication protocols. Unfortunately, personal data, including Social Security numbers, may have been compromised, according to the recent news.

As this case shows, personal data and system protocols can be damaged in the same event. Incidents like this one are worthy of being analyzed not from two different views, but from a combined perspective that includes data protection and cybersecurity, because data breaches affect various aspects of an organization’s life cycle, the response should be multilateral. In other words, both cybersecurity and data protection specialists should combine their skills to prevent data breaches.” [14]

Here are some of the advantages of combining data protection with cybersecurity. Let’s look at the details.

• **Prevent data breaches.** Overseeing both data and systems at the same time leaves less space for vulnerabilities and exploits.

• **Address emerging digital threats.** There are digital threats that pose a risk for both data and systems.

• **Enhance your information security management system (ISMS).** Having a single pane of glass ISMS allows you to control your data better than with separate infrastructure for data protection and cybersecurity.

• **Improve compliance.** Reducing the probability of a data breach helps you to stay compliant and avoid compliance violation penalties.

Both data protection and cybersecurity deal with protecting sensitive data from various digital threats. That’s why they have become interconnected. Rather than having them respond to a breach separately, it makes sense to have one integrated approach.

ACKNOWLEDGMENT

The preparation of this paper has been facilitated by discussions with experts, including some master's students, and reference to access to study material in Metropolia and other sites.

REFERENCES

[1] FSB, "Why is data protection so important?," FSB, 5 October 2019. [Online]. Available: https://www.fsb.org.uk/resources-page/why-is-data-protection-so-important.html#:~:text=Key%20pieces%20of%20information%20that,phishing%20scams%2C%20and%20identity%20theft.. [Accessed 02 Decemeber 2020].

[2] J. B. Neto, "Arquivo para a página," 15 March 2013. [Online]. Available: https://commons.wikimedia.org/wiki/File:Data_types_-_pt_br.svg#file. [Accessed 01 Decemeber 2020].

[3] G. Greenleaf, "Global Data Privacy Laws: 89 Countries, and Accelerating," 6 February 2012. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000034. [Accessed 01 December 2020].

[4] D. Walker and I. T.Pro, "What is the Data Protection Act 1998?," 2019. [Online]. Available: https://search-proquest-com.ezproxy.metropolia.fi/magazines/what-is-data-protection-act-1998/docview/2243861188/se-2?accountid=11363.. [Accessed 01 Decemeber 2020].

[5] Official Journal of the European Union, "General Data Protection Regulation," 27 April 2016. [Online]. Available: https://gdpr-info.eu/. [Accessed 01 December 2020].

[6] javatpoint, "Cyber Security Tutorial," 2018. [Online]. Available: https://www.javatpoint.com/cyber-security-tutorial. [Accessed 28 November 2020].

[7] Digital Defense Inc., "What is Cybersecurity & What Does it Really Mean?," Digital Defense, Inc., [Online]. Available: https://www.digitaldefense.com/blog/what-is-cybersecurity-what-does-it-really-mean/. [Accessed 29 November 2020].

[8] PR Newswire; New York, "Cyber Security Cloud Releases Research Report on Personal Data Breach Incidents due to Unauthorized Access from October 2019 to September 2020: Cyber Security Cloud, Inc.," 5 October 2020. [Online]. Available: https://search-proquest-com.ezproxy.metropolia.fi/docview/2451131854/fulltext/70C3C242E0074564PQ/1?accountid=11363. [Accessed 25 November 2020].

[9] verizon, "2020 Data Breach Investigations Report," 2020. [Online]. Available: https://enterprise.verizon.com/resources/reports/dbir/. [Accessed 01 December 2020].

[10] D. Swinhoe, "The 15 biggest data breaches of the 21st century," CSO, 17 April 2020. [Online]. Available: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html. [Accessed 25 November 2020].

[11] L. ODonnell, "Vastaamo Breach: Hackers Blackmailing Psychotherapy Patients," 26 October 2020. [Online]. Available: https://search-proquest-com.ezproxy.metropolia.fi/blogs,-podcasts,-websites/vastaamo-breach-hackers-blackmailing/docview/2454168584/se-2?accountid=11363. . [Accessed 1 December 2020].

[12] J. Fruhlinger, "Top cybersecurity facts, figures and statistics for 2020," CSO, 9 March 2020. [Online]. Available: https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html. [Accessed 01 December 2020].

[13] T. Vihermaa., *Trends in ICT*, Espoo: nixu cybersecurity[unpublished lecture notes], 2020.

[14] D. Dontov, "Why Data Protection And Cybersecurity Can't Be Separate Functions," YECCOUNCIL POST, [Online]. Available: https://www.forbes.com/sites/theyec/2020/11/25/why-data-protection-and-cybersecurity-cant-be-separate-functions/?sh=2a38a66c17cc. [Accessed 01 December 2020].