10. DATA ETHICS AND INFORMATION SECURITY

Author: Dario Šebalj

In the era of digital transformation, the ethical handling and security of data have emerged as major issues for individuals and organizations. As vast amounts of personal and sensitive information are collected and processed daily, ensuring that this data is managed responsibly and securely is very important.

This chapter examines the principles of data ethics, highlighting the moral considerations and best practices for data handling, and explores the various threats to information security. By understanding and addressing these issues, we can protect privacy, maintain trust, and foster a safer digital environment.

10.1. The importance of data ethics

Data ethics refers to the moral principles and practices guiding the collection, processing, sharing, and utilization of data to ensure respect for individuals' rights, societal well-being, and trust. It encompasses transparency, accountability, fairness, and privacy, ensuring that data practices are aligned with ethical standards and legal frameworks to prevent harm and promote responsible innovation (Cognizant, n.d.; Gov.uk, 2020; Knight, 2021; McKinsey, 2022; Cepelak, 2023).

In today's digital landscape, the ethical handling of data is crucial for maintaining trust and securing a competitive edge. The McKinsey (2022) article on data ethics highlights the importance of integrating ethical considerations into data management practices. It points out three common mistakes: assuming data ethics are irrelevant, relying solely on legal and compliance teams for oversight, and prioritizing short-term financial gains over ethical practices. To address these issues, they recommend several strategies. First, companies should establish clear, company-specific guidelines for data ethics. These guidelines serve as a foundation for ethical data management and help in setting

a standard across the organization. Second, forming diverse teams to handle data-related issues ensures a range of perspectives and reduces the risk of biased decision-making. Third, involving senior leadership as champions of data ethics initiatives is crucial for driving these practices throughout the organization.

Figure 10.1 5C of Data Ethics

Source: Author, adapted from Atlan (2023).

Figure 10.1 shows 5C of Data Ethics, outlined by Atlan (2023), which represents essential principles for ethical data handling:

- **Consent:** Obtain informed, voluntary consent from individuals before collecting their data, ensuring transparency about data usage.
- **Collection:** Only collect data necessary for specific purposes, avoiding excessive data collection.
- **Control:** Allow individuals to access, review, and update their data, ensuring they have control over its use.
- **Confidentiality:** Protect data from unauthorized access and breaches through robust security measures.
- **Compliance:** Adhere to legal and regulatory requirements, conducting regular audits to ensure ongoing compliance.

Similar to Atlan's principles, Cote (2021) identifies five core principles of data ethics that are essential for business professionals to uphold:

- **Ownership** emphasizes that individuals retain ownership over their personal information. It is both unlawful and unethical to collect personal data without explicit consent. Companies must obtain consent through clear agreements or digital privacy policies, ensuring that users are aware and agree to data collection practices.
- **Transparency** involves clear communication regarding how data will be collected, stored, and used. Businesses must inform individuals about the methods and purposes of data collection. This transparency builds trust and allows users to make informed decisions about their data. Deceptive practices or withholding information about data usage are both unethical and unlawful.
- **Privacy** focuses on the responsibility of businesses to protect the privacy of personal information. Even with consent, personal data should not be made publicly available without the individual's explicit permission. Companies must implement robust security measures to safeguard personal information from unauthorized access or breaches.
- **Intention** pertains to the ethical motivations behind data collection and usage. Data should be collected and used for purposes that are beneficial and not harmful to individuals or society. Ethical data practices involve using data to enhance user experiences and improve services without exploiting or causing harm.
- **Outcome** considers the broader impacts of data usage on individuals and society. Businesses must evaluate the potential consequences of their data practices and strive to avoid negative outcomes. This principle emphasizes the need for ethical foresight and responsibility in data-driven decision-making.

Guzman & Dyer (2020) emphasize that ethical challenges in data practices are not straightforward and often lack clear-cut solutions. They stated that there is a discrepancy between ethical expectations online and offline. Many individuals perceive a form of exceptionalism in online spaces, where traditional ethical rules do not seem to apply. This mindset can lead to the justification of actions online that would be deemed unethical offline. Authors are proposing an ethical approach that bridges both realms, emphasizing that ethical principles should remain consistent regardless of the medium.

The paper on data ethics published by Basl et al. (2021) explores the complex process of moving from abstract ethical principles to concrete, implementable promises in the context of big data and artificial intelligence (AI). They concluded that it is difficult and important

to make this shift in order to guarantee that ethical behaviour is not just theoretical but also practical and significant.

According to O'Reilly (2018), four anonymized case studies have been developed by Princeton's Centre for Information Technology Policy and Centre for Human Values to encourage ethical discourse. One of the case studies explores the ethical dilemmas posed by an automated healthcare app designed to assist adult-onset diabetes patients using AI. It underscores the need to balance technological benefits with ethical principles such as autonomy, fairness, and accountability. Addressing these ethical challenges is crucial for the responsible integration of AI in healthcare, ensuring that it serves the best interests of all patients. There are some key issues that need to be addressed:

- **Paternalism:** The app aims to encourage healthier behaviours among patients by nudging them towards better choices. While this can improve health outcomes, it raises ethical questions about autonomy and paternalism. Is it ethical for the app to influence patient behaviour, or should patients have complete autonomy over their health decisions?
- **Consent and transparency:** The app collects sensitive health data to function effectively. Ensuring informed consent and transparency about data collection, usage, and sharing is crucial. Patients must be fully aware of what data is being collected, how it will be used, and who will have access to it.
- **Data privacy and security:** Handling sensitive health data requires stringent privacy and security measures. The case study emphasizes the need for robust data protection protocols to safeguard patient information from breaches and unauthorized access.
- **Responsibility and accountability:** Determining who is responsible for the app's decisions and actions is another critical aspect. If the app makes an incorrect recommendation that adversely affects a patient's health, identifying the responsible party (developers, healthcare providers, or the app itself) is complex but necessary for accountability.

Modern data management is fundamentally based on data ethics, which guarantees fair, transparent, accountable, and privacy-respecting data practices. Organizations can foster responsible innovation, avoid legal pitfalls, and increase trust by upholding ethical standards. It is not only a best practice but also a requirement for sustainable and responsible growth to

incorporate strong ethical frameworks into data management practices as data becomes more and more essential to operations and decision-making.

Another important aspect is information security since data ethics and information security are intrinsically linked. Ensuring ethical data practices lays the foundation for robust information security measures. Protecting data from unauthorized access, breaches, and other security threats not only preserves privacy and confidentiality but also upholds the ethical principles discussed in this chapter.

10.2. Fundamentals of information security

Information security refers to the comprehensive set of practices and principles aimed at safeguarding information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. It ensures the confidentiality, integrity, and availability of data through the implementation of protective measures, policies, and technologies. These measures include access control, encryption, disaster recovery, and compliance with legal and regulatory standards to mitigate risks and protect against potential threats (Fruhlinger, 2020; CISCO, n.d., NIST, n.d.).

Information security is now essential to an organization's credibility and integrity in the digital era. Its importance is highlighted by the growing dependence on digital data and the rise in cyberthreats that compromise sensitive data. First and foremost, information security protects sensitive data from unauthorized access, breaches, and theft. This includes personal information, financial data, intellectual property, and confidential business communications. As cyberattacks become more sophisticated, the risk of data breaches escalates, potentially leading to severe financial losses and reputational damage. For instance, the 2017 Equifax breach exposed the personal information of 147 million people, resulting in a settlement of up to $425 million (Federal Trade Commission, 2022). Such incidents highlight the dire consequences of inadequate information security measures.

Furthermore, information security is critical for retaining consumer trust and confidence. In an age when data privacy is crucial, customers are becoming more concerned about how their information is handled. A strong information security architecture ensures that consumers' data is secure, which fosters loyalty and trust. According to an IBM survey, **75%**

of customers would not buy from a firm that they do not trust to preserve their data (PR Newswire, 2018). Thus, information security is both a technological need and a strategic business imperative.

Information security is also critical for mitigating operational disturbances. Cyberattacks, such as ransomware, may disrupt corporate operations by preventing users from accessing essential systems until a ransom is paid. The 2021 Colonial Pipeline ransomware attack, which led to fuel shortages across the eastern United States, exemplifies the disruptive potential of such threats (Kerner, 2022). By implementing strong security measures, organizations can safeguard their operational continuity and resilience against such disruptions.

According to Kim and Solomon (2018), information is considered secure if it meets three major tenets:

- **confidentiality:** sensitive information is accessed only by authorized individuals,
- **integrity:** information can only be altered by those with permission,
- **availability:** information and resources are accessible to authorized users whenever needed.

Those tenets are often called CIA triad, as shown in Figure 10.2.

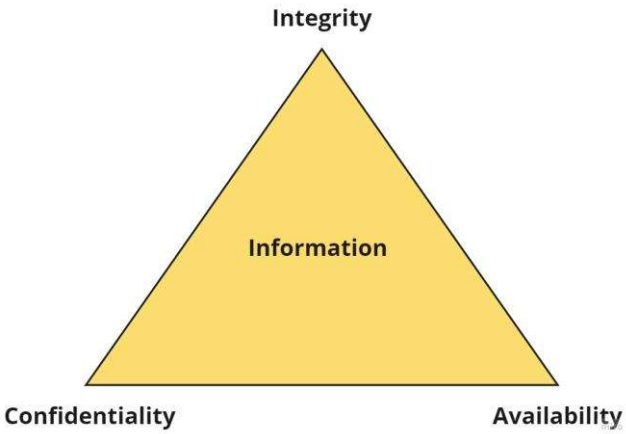

Figure 10.2 The CIA triad

Source: Author, adapted from Kim and Solomon (2018).

In information security, the concepts of risk, threat, and vulnerability are central to understanding and managing security. **Risk** is the likelihood that something bad will happen to an asset. In information security, risk is the probability of a harmful event affecting

the confidentiality, integrity, or availability of information. For example, a company might assess the risk of a cyber-attack on its network by considering both the likelihood of such an attack and the potential damage it could cause. A threat is any action that has the potential to cause harm to information systems or data. **Threats** can be intentional, such as cyber-attacks by hackers, or unintentional, such as natural disasters or human error. **Vulnerability** refers to weaknesses or gaps in a system's defence that can be exploited by threats to cause harm. These can be flaws in software, hardware, organizational processes, or human behaviour (Kim and Solomon, 2018).

To effectively protect information systems, organizations need to understand how risks, threats, and vulnerabilities interact. For instance, a vulnerability in software (such as a security flaw) might be exploited by a threat actor (such as a hacker), leading to a data breach, which constitutes a risk to the organization. By identifying and mitigating vulnerabilities, organizations can reduce the risk of threats causing significant damage.

10.2.1. Data breaches

Data breaches have become a significant threat in the digital age, affecting organizations across various sectors. These breaches compromise sensitive information, leading to financial losses, reputational damage, and legal consequences. Understanding the magnitude and impact of data breaches is crucial for developing effective security strategies to protect against such incidents. According to Fortinet (n.d.), a **data breach** "is an event that results in confidential, private, protected, or sensitive information being exposed to a person not authorized to access it". These breaches can happen in various ways (Kaspersky, n.d.a):

1. **Accidental insider:** An employee unintentionally accesses sensitive information without proper authorization. For example, using a colleague's computer and viewing confidential files.
2. **Malicious insider:** An individual with authorized access intentionally misuses data for harmful purposes. This could involve stealing or leaking sensitive information.
3. **Lost or stolen devices:** Unencrypted and unsecured devices such as laptops or external drives containing sensitive data are lost or stolen, making the information vulnerable to unauthorized access.

4. **Malicious outside criminals:** Hackers use various methods to breach systems, including phishing attacks, brute force attacks, and malware. These cybercriminals exploit vulnerabilities in software, networks, and user behaviour to gain access to sensitive data.

According to Kaspersky (n.d.a), common methods used in data breaches include **phishing**, where cybercriminals impersonate trusted entities to trick individuals into divulging sensitive information. Another method is **brute force attacks**, where hackers use software to repeatedly guess passwords, exploiting weak or reused credentials to gain unauthorized access to accounts. Additionally, **malware**, such as spyware, is used to infiltrate systems and steal data undetected. These methods will be explained later in the chapter.

Human error accounts for **95%** of all data breaches (Cybernews, 2022).

The 21st century has witnessed some of the most severe data breaches, highlighting the vulnerabilities in digital systems and the critical need for robust security measures. According to Hill and Swinhoe (2022) and ESET (n.d.), there are some of the most notable data breaches:

- **Yahoo (2013-2014):** Yahoo experienced one of the largest data breaches in history, with all three billion of its user accounts compromised in 2013. This breach exposed names, email addresses, dates of birth, and security questions and answers. Another breach in 2014 affected 500 million accounts, further highlighting the company's security vulnerabilities.
- **Marriott International (2018):** Marriott announced a breach affecting approximately 500 million guests. Hackers had access to the Starwood guest reservation database, exposing personal information such as names, addresses, phone numbers, email addresses, and passport numbers. This breach was a result of unauthorized access dating back to 2014. The Information Commissioner's Office (ICO), a UK data regulatory authority, ultimately fined the corporation £18.4 million in 2020 for failing to protect the privacy of its customers' personal information.

- **Adult Friend Finder (2016):** The Adult Friend Finder breach exposed the personal information of 412 million accounts, including names, email addresses, and passwords, many of which were poorly encrypted. This incident raised significant concerns about the security practices of online platforms handling sensitive personal information.
- **MySpace (2013):** The MySpace data breach, which occurred in 2013, resulted in the exposure of over 360 million user accounts. The data included names, email addresses, and passwords. Hackers later sold this information on the dark web, which highlighted the vulnerabilities in the security systems of social media platforms during that time.
- **LinkedIn (2021):** In 2021, personal data of 700 million LinkedIn users was posted on a dark web forum. The hacker used data scraping techniques via LinkedIn's API to obtain email addresses, phone numbers, and other personal details. Although not a traditional hack, this incident raised serious concerns about data privacy and the potential misuse of scraped data for social engineering attacks.
- **Equifax (2017):** This breach exposed the personal data of nearly 148 million Americans, 15.2 million Brits, and 19,000 Canadians. Hackers exploited a vulnerability in the Apache Struts web application framework that Equifax had failed to patch. The stolen data included social security numbers, birth dates, and addresses, leading to an estimated $1.7 billion in costs for Equifax.
- **eBay (2014):** eBay disclosed a breach that affected 145 million users. The attack originated from compromised employee login credentials, leading to the exposure of names, email addresses, physical addresses, phone numbers, and encrypted passwords. This breach highlighted vulnerabilities in employee access controls and the importance of strong authentication measures.
- **Target (2013):** A breach affecting over 41 million payment card accounts and the contact information of more than 60 million customers. Cybercriminals accessed customer data, including names, phone numbers, email addresses, credit and debit card numbers, and encrypted PINs. Target faced substantial legal and settlement costs, including a $10 million class-action lawsuit and an $18.5 million multistate settlement.

These breaches demonstrate the far-reaching consequences of cyberattacks and the critical need for strong cybersecurity practices. By learning from these high-profile cases, organizations can better protect their data, improve their security protocols, and minimize

the risk of future breaches. Data breaches are often the result of a range of underlying threats. Understanding these threats is critical to building successful information security measures. Cyber threats may emerge from a variety of sources, including malicious insiders, cybercriminals, and even state-sponsored actors. In addition, vulnerabilities in systems and networks may be exploited to get unauthorized access to sensitive information.

10.2.2. Information security threats

Security threat is a malicious act that attempts to corrupt or steal data, compromise an organization's systems, or compromise the company as a whole (TechTarget, 2024). There are many different information security threats that seriously jeopardize data availability, integrity, and confidentiality.

According to Kim and Solomon (2018) and Grubb (2021), **malware** (malicious software) is designed to infiltrate, damage, or disable computers and networks. Common types of malware include viruses, worms, trojans, ransomware, and spyware. A **virus** is a type of malware that attaches itself to a legitimate programme or file and spreads to other programmes and files when the infected software is executed. Viruses can corrupt or delete data, disrupt system operations, and spread to other systems through email attachments, network connections, or removable media. Unlike viruses, **worms** are standalone malware that can self-replicate and spread independently across networks without needing to attach to a host programme. Worms exploit vulnerabilities in operating systems or applications to propagate, often causing network congestion and overloading systems by consuming bandwidth and resources. A **trojan**, or trojan horse, is malware disguised as legitimate software. Users are tricked into installing it, believing it is a harmless or useful programme. **Ransomware** is a type of malware that encrypts the victim's data, rendering it inaccessible until a ransom is paid to the attacker. Ransomware attacks can be devastating, leading to significant data loss and operational disruption if the ransom is not paid or backups are not available. **Spyware** is malware designed to gather information about a person or organization without their knowledge. It can collect various types of data, such as keystrokes, browsing habits, and personal information, and transmit this data to a third party.

Another type of threat is **phishing**. Kosinski (2024) explains that phishing attacks involve fraudulent emails, texts, calls, or websites designed to deceive individuals into disclosing

personal information or downloading malware. These attacks exploit human error and trust, making them highly effective. To combat phishing, organizations must use advanced threat detection tools and provide robust employee training to recognize and respond to these scams effectively.

Phishing is the leading cause of data breaches, accounting for 16% and costing organizations an average of **$4.76 million** per breach (Kosinski, 2024).

There are four main types of phishing (Forbes, 2024):

- **Email phishing:** using email to steal sensitive information. Attackers may target large audiences by assuming the identity of reputable organizations.
- **Spear phishing:** sending individualized emails, texts, or phone calls with the intent of gaining access to computer systems or sensitive information. When using this technique, attackers usually use data from open databases, social media, or past breaches to bolster their legitimacy.
- **Whaling:** it focuses on high-ranking or senior personnel, including finance officers and chief executives. Attackers create very convincing, highly tailored communications to get sensitive data and information from a business.
- **Vishing:** making phone calls or leaving voicemails under the guise of a reliable source. The goal is to get bank accounts, take advantage of personal information, and steal money.

Insider threats are security risks that originate from within the organization. They can be employees, contractors, or business partners who have access to the organization's systems and data. These threats can be particularly dangerous because insiders often have legitimate access to sensitive information and systems, making their malicious activities harder to detect (TechTarget, 2024).

Another type of threat are **Distributed Denial-of-Service** (DDoS) attacks. They aim to disrupt the normal traffic of a targeted server, service, or network by overwhelming it with a flood of internet traffic. This is achieved by using multiple compromised computer systems as sources of attack traffic. When these devices, often distributed globally, simultaneously

send numerous requests to the target, they consume its available bandwidth and resources, leading to service outages and preventing legitimate users from accessing the service (TechTarget, 2024).

Internet security threats are closely tied to the actions of hackers, who exploit vulnerabilities in systems for various malicious purposes. According to Grubb (2021), hackers are often categorized based on their intentions and methods. Two primary categories are white hat hackers and black hat hackers. **White hat hackers**, also known as ethical hackers, use their skills for defensive purposes. They work to protect organizations from cyber threats by identifying and fixing security vulnerabilities before malicious hackers can exploit them. **Black hat hackers**, in contrast, engage in illegal activities with malicious intent. They exploit security vulnerabilities for personal gain, which can include stealing data, spreading malware, or causing disruptions.

One crucial defence against information security threats is the use of strong passwords. Strong passwords, which should be complex and unique for each account, significantly reduce the risk of unauthorized access.

Table 10.1 shows the time it takes a hacker to brute force a password, according to research conducted by Hive Systems (2024).

Table 10.1 Time it takes a hacker to brute force a password in 2024

Number of characters	Numbers only	Lowercase letters	Upper and lowercase letters	Numbers, upper and lowercase letters	Numbers, upper and lowercase letters, symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 min	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652 bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

Source: Author, adapted from Hive Systems (2014).

Understanding the various types of information security threats, such as phishing attacks, malware, and DDoS attacks, highlights the critical need for robust cybersecurity measures. These threats pose significant risks to personal data, financial information, and organizational integrity. Because of this, it becomes essential to adopt comprehensive security strategies. The following sub-chapter presents suggestions for maintaining strong internet security, including practical tips that people and institutions can use to protect their digital resources.

10.2.3. Information security recommendations

Large number of security risks, such phishing and malware, can be greatly minimized by understanding them and putting them into practice. There are several most important recommendations for ensuring information security (Rubenking & Duffy, 2023; NSW Government, n.d.; Kaspersky, n.d.b):

- **Use strong passwords:** create complex passwords combining letters, numbers, and symbols for each account. Avoid using easily guessable information like birthdays. Use a password manager to store and manage your passwords securely.

- If possible, **enable multi-factor authentication (MFA):** add an additional layer of security by requiring two or more verification methods to access your accounts, such as a password and a one-time code sent to your phone.
- **Keep software updated:** regularly update your operating systems, browsers, and applications to patch security vulnerabilities. Enable automatic updates whenever possible to ensure you are always protected against the latest threats.
- **Be aware of phishing scams:** do not click on links or download attachments from unknown or suspicious emails. Verify the sender's information and look for signs of phishing, such as misspellings or urgent requests for personal information.
- **Use secure connections:** ensure your internet connection is secure by using Virtual Private Networks (VPNs) and avoiding public Wi-Fi for sensitive activities like online banking. Check for "https://" in the URL, indicating a secure connection.
- **Backup data regularly:** regularly back up your data to external drives or cloud storage services. This practice ensures you can recover your information in case of hardware failure, theft, or a ransomware attack.
- **Install antivirus software:** use reputable security software to detect, prevent, and remove malware. Keep your antivirus software updated and perform regular scans to ensure your system is clean.
- **Monitor accounts regularly:** frequently check your financial and online accounts for any unauthorized activities. Set up alerts for unusual transactions and report any suspicious behaviour immediately to your service provider.

By understanding the ethical implications of data handling and recognizing the security threats that exist, individuals and organizations can develop effective strategies to protect sensitive information. From establishing ethical guidelines and using strong, unique passwords to implementing advanced security measures and staying informed about potential threats, these practices collectively ensure the integrity, confidentiality, and availability of data. By prioritizing data ethics and robust security protocols, a safer, more trustworthy digital environment can be created.

REFERENCES

1. Atlan (2023). Data Ethics Unveiled: Principles & Frameworks Explored [available at: https://atlan.com/data-ethics-101/, access May 17, 2024]
2. Basl, J., Sandler, R. & Tiell, S. (2021). Getting from commitment to content in AI and data ethics: Justice and explainability. Atlantic Council [available at: https://www.atlanticcouncil.org/in-depth-research-reports/report/specifying-normative-content/, access May 17, 2024]
3. Cepelak, C. (2023). What is Data Ethics? Datacamp [available at: https://www.datacamp.com/blog/introduction-to-data-ethics, access May 14, 2024]
4. CISCO (n.d.). What Is Information Security? [available at: https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html, access May 20, 2024]
5. Cognizant (n.d.). Data ethics [available at: https://www.cognizant.com/us/en/glossary/data-ethics, access May 14, 2024]
6. Cote (2021). 5 Princples of Data Ethics for Business. Harvard Business School Online [available at: https://online.hbs.edu/blog/post/data-ethics, access May 17, 2024]
7. Cybernews (2022). World Economic Forum finds that 95% of cybersecurity incidents occur due to human error [available at: https://cybernews.com/editorial/world-economic-forum-finds-that-95-of-cybersecurity-incidents-occur-due-to-human-error/, access May 21, 2024]
8. ESET (n.d.). 5 scary data breaches that shook the world [available at: https://www.eset.com/in/about/newsroom/corporate-blog/corporate-blog/eset-5-scary-data-breaches-that-shook-the-world/, access May 21, 2024]
9. Federal Trade Commission (2022). Equifax Data Breach Settlement [available at: https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement, access May 20, 2024]
10. Forbes (2024). Cybersecurity Stats: Facts And Figures You Should Know [available at: https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/, access May 24, 2024]

11. Fortinet (n.d.). What Is A Data Breach? [available at: https://www.fortinet.com/resources/cyberglossary/data-breach, access May 21, 2024]
12. Fruhlinger, J. (2020). What is information security? Definition, principles, and jobs. CSO [available at: https://www.csoonline.com/article/568841/what-is-information-security-definition-principles-and-jobs.html, access May 20, 2024]
13. Gov.uk (2020). Data Ethics Framework: glossary and methodology [available at: https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework-glossary-and-methodology, access May 14, 2024]
14. Grubb, S. (2021). How Cybersecurity Really Works: A Hands-on Guide for Total Beginners. No starch press.
15. Guzman, L. & Dyer, S. (2020). Ten questions we're asking about ethics, data, and open source research. Amnesty International [available at: https://citizenevidence.org/2020/11/10/ethics-data-open-source/, access May 17, 2024]
16. Hill, M. & Swinhoe, D. (2022). The 15 biggest data breaches of the 21st century. CSO Online [available at: https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html, access May 21, 2024]
17. Hive Systems (2024). Are Your Passwords in the Green? [available at: https://www.hivesystems.com/blog/are-your-passwords-in-the-green?utm_source=tabletext, access May 24, 2024]
18. Kaspersky (n.d.a). How Data Breaches Happen & How to Prevent Data Leaks [available at: https://www.kaspersky.com/resource-centre/definitions/data-breach, access May 21, 2024]
19. Kaspersky (n.d.b). Top 15 internet safety rules and what not to do online [available at: https://www.kaspersky.com/resource-centre/preemptive-safety/top-10-preemptive-safety-rules-and-what-not-to-do-online, access May 25, 2024]
20. Kerner, S. M. (2022). Colonial Pipeline hack explained: Everything you need to know. TechTarget [available at: https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know, access May 20, 2024]

21. Kim, D. & Solomon, M. G. (2018). Fundamentals of Information Systems Security, 3rd Edition. Jones & Bartlett Learning.
22. Knight, M. (2021). What Is Data Ethics?. Dataversity [available at: https://www.dataversity.net/what-are-data-ethics/, access May 14, 2024]
23. Kosinski, M. (2024). What is a phishing attack? IBM [available at: https://www.ibm.com/topics/phishing, access May 24, 2024]
24. McKinsey (2022). Data ethics: What it means and what it takes [available at: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/data-ethics-what-it-means-and-what-it-takes, access May 14, 2024]
25. National Institute of Standards and Technology (NIST) (n.d.). Information security [available at: https://csrc.nist.gov/glossary/term/information_security, access May 20, 2024]
26. NSW Government (n.d.). 10 Tips for Cyber Security [available at: https://www.digital.nsw.gov.au/sites/default/files/2022-09/top-10-cyber-security-tips.pdf, access May 25, 2024]
27. O'Reilly (2018). Case studies in data ethics [available at: https://www.oreilly.com/content/case-studies-in-data-ethics/, access May 17, 2024]
28. PR Newswire (2018). New Survey Finds Deep Consumer Anxiety over Data Privacy and Security [available at: https://www.prnewswire.com/news-releases/new-survey-finds-deep-consumer-anxiety-over-data-privacy-and-security-300630067.html, access May 20, 2024]
29. Rubenking, N. J. & Duffy, J. (2023). 12 Simple Things You Can Do to Be More Secure Online. PC mag [available at: https://www.pcmag.com/how-to/12-simple-things-you-can-do-to-be-more-secure-online, access May 25, 2024]
30. TechTarget (2024). Top 10 types of information security threats for IT teams [available at: https://www.techtarget.com/searchsecurity/feature/Top-10-types-of-information-security-threats-for-IT-teams, access May 24, 2024]