Cybersecurity on the Edge?

Abstract

As often encountered in life, we are faced with a trade-off: on the one hand the opportunities afforded from communications networks, services and end-user devices are seemingly endless, but on the other hand, our reliance on them has proven to be an attractive target for cyber criminals to cause disruption. The risk becomes greater when the technology falls short on cybersecurity. This essay recognises there are no silver bullets preventing all cyber-attacks and data breaches, but it looks at the various means to minimise the risks of exposure to them. I argue that governments are taking proactive steps in establishing what good cybersecurity practices should look like, and industry has more incentives than ever to ensure cybersecurity is not neglected. However, security is only as strong as the weakest link, so fostering a shared sense of responsibility to act on cybersecurity, both at the individual and organisational level, are paramount.

Cybersecurity – a long underrated practice is now in the spotlight

Cybersecurity is broadly defined as the steps taken by individuals and organisations to reduce the risk of a cyber-attack, a scenario in which an individual or group gains access to computer systems, networks and computer data for malicious intent, thereby compromising the integrity, confidentiality, or availability of that data[1]. The steps have a dual function of protecting devices we use and services we access, as well as preventing unauthorised access to the vast amounts of data, including personal information, we store on our devices and online (National Cyber Security Centre (NCSC), n.d.).

Protecting our information is not new to the digital age – the practice has long been known as information security. Whereas information security aims to protect both forms of physical and digital data from unauthorised access, cybersecurity is chiefly concerned with protecting data hosted in the cyber domain. In simple terms, cybersecurity is a subset of information security.

As technology evolves, so does the risk of cyber-attacks

Before personal computers became mainstream and connected to the Internet in masses, cybersecurity could have been considered a niche profession, with cybersecurity incidents possibly deemed to be less of a concern. However, in recent years, the global importance of cybersecurity has been reflected in news headlines. I believe two trends are contributing to these events.

[1] Known as the "CIA triad".
Confidentiality: data should not be accessed without authorisation,
Integrity: data should not be tampered with, and
Availability: data should be available when requested to those with authorised access.

Firstly, we live in times where the number of end-user devices connected to the Internet comfortably surpasses the global population (Cisco, 2020). A recent study estimates a household in the United States (US) owns on average 20.2 connected devices[2], and 17.4 and 10.3 in Europe and Japan, respectively (Koetsier, 2022)[3]. The reality is that for every additional connected gadget we embrace, we open the door to a new vector of attack, a way for a malicious actor to enter a network or system and exploit it. Weak and default passwords as well as lack of continued security updates are just two of the common vulnerabilities found in "smart" toys and home appliances such as teddy bears[4] and doorbell cameras[5].

Secondly, the communications networks connecting the above-mentioned end-user devices are becoming increasingly interdependent and complex. 5G, which has now been deployed in over 94 markets worldwide (Standard and Poor, 2023), is promising faster connectivity and lower latency[6] making it apt for industrial usage and "connected everything". Cloud computing and multi-access edge computing (MEC) are playing a key role in 5G deployments helping operators meet, manage, and optimise the demands on their networks, accelerating their virtualisation and softwarisation[7]. Whilst cloud and MEC solutions offer security benefits, integrating them into the network architecture can result in new vectors of cyber-attacks (Organisation for Economic Co-operation and Development (OECD), Forthcoming). For their part, communications providers are also having to deal with increasingly complex network configurations that need constant monitoring, a task that becomes more challenging as they expand.

Additionally, as the number of devices we use increases, and the technology that connects them evolves, we are witnessing a more complex cyber threat landscape whereby ransomware, malware and social engineering tactics are becoming prominent techniques for cyber-attackers (European Union Agency for Cybersecurity (ENISA), 2022). The fact that tensions between countries have been exported to the cyber domain is exacerbating this trend. Nation State actors[8] are even resorting to using criminal organisations to deploy malicious cyber campaigns with societal and financial impacts of varying degrees (Center for Strategic and International Studies, n.d.).

Privacy: one of the most important consumer protection issues is related to the security of a system or device

Debates about the trade-offs between privacy and security are common nowadays, but this essay views these concepts as closely linked[9]. As indicated earlier, cybersecurity measures are not only

[2] Connected devices referred to in broad terms: Internet of Things devices ("smart devices") as well other devices such as smartphones, computers, tablets and laptops.
[3] Whilst the statistics may heavily represent countries where ownership of devices and access to connectivity are mostly privileged, all countries are exposed to cyber threats and as lesser developed countries catch-up, so will the prominence of these threats.
[4] The Guardian, Fisher-Price smart bear allowed hacking of children's biographical data, 2016.
[5] NCC Group, Domestic IoT Nightmares: Smart Doorbells, 2020.
[6] Latency is the time it takes for data to pass from one point on a network to another.
[7] In simple terms, it refers to the decoupling of hardware from software in a network allowing key network functions to become software based.
[8] Individuals or groups who are sponsored by a government to conduct cyber-attacks against other countries or organisations.
[9] For instance, much of the privacy versus security debate today is centred around end-to-end encryption, namely in the United Kingdom and the European Union on proposed legislation to combat child sexual material online in messaging platforms. Some advocate that lawful access to end-to-end encryption messages should be allowed in cases of child sexual abuse and national security concerns (e.g., terrorism),

important to protect the networks and devices we use, but also the personal and sensitive information they hold. When considering the three pillars of security outlined above – confidentiality, integrity and availability – it helps to view privacy and confidentiality as intertwined. Privacy refers to the right to manage and control personal information and keep it confidential (Norton, 2021). It is possibly one of the most important consumer protection issues of our times, with one recent survey finding that nearly 70% of consumers globally are either somewhat or very concerned about their privacy online (The International Association of Privacy Professionals , 2023). This is particularly telling considering Internet users globally spend over six hours online per day (Meltware and We Are Social, 2023). The information we submit when we sign up to online services or accounts is usually managed through privacy policies, which govern how a website or an application collects and handles our personal data. Having a privacy policy has become a legal requirement in many countries for businesses and organisations collecting personal data[10]. Complementary to privacy policies, data security policies set out the controls an organisation implements to protect the data from unauthorised access. A service that collects our personal information, whether it be an email address, passport credentials or credit card details, can be targeted by cyber criminals. When a cybersecurity incident occurs, it can often lead to a privacy breach[11], whereby cyber criminals get access to personal information for the purpose of selling or using this stolen data to attempt identity or financial theft [12].

In an era of rapid technological evolution, where a large part of our society relies on networks and devices and values privacy, cybersecurity should be at the core of every network or product deployed into the market. Paradoxically, this has not been the case, requiring several high-profile cybersecurity incidents, including privacy breaches, to bring attention to this problem.

How governments and the private sector are responding to the threat landscape and their shared responsibility in promoting increased levels of cybersecurity

From a tech issue to a public interest and national security concern: cybersecurity becomes a priority in governmental agendas

Developing a framework guiding a national cybersecurity posture has been high on many governments' agenda. A survey of 194 countries conducted in 2020 found that 127 countries have published or are in the process of drafting a national cybersecurity strategy (International Telecommunications Union, 2021). Faced with increasing cyber-attacks and an evolving cyber threat landscape, governments and regulators around the world have taken more assertive stances in relation to what they expect good cybersecurity should look like. This is evidenced not only by the release of joint recommendations from national cybersecurity agencies urging

and others argue that encryption is fundamental to protect users' privacy and "backdoors" to encryption would weaken security protections.

[10] With the General Data Protection Regulations (GDPR) as a main example.

[11] The term "privacy breach" instead of "data breach" is deliberate to emphasise the loss of confidentiality and control over data.

[12] This information can be sold on the dark web, a hidden part of the Internet that is not accessible through common web browsers and may be used by people to carry out illegal activities.

industry to take more action[13], but also by the rising trend in legislating and regulating for specific outcomes or rules to which the industry is expected to conform.

On the networks side, governments are announcing new measures in recognition of networks being essential to society's functioning and of new mobile generations (such as 5G and eventually 6G) underpinning most sectors of the economy in the future. In some cases, these are also driven by the desire to protect networks from foreign interference of countries deemed to pose national security concerns. Such measures include the implementation of technical requirements that would apply to major, if not all, communications providers (e.g., the Netherlands[14], Singapore[15], the United Kingdom[16]) or pre-authorisation or screening regimes for some network equipment (e.g., France[17], Australia[18], India[19]). Along with new measures, governments are also extending laws governing the security of national critical infrastructure to encompass communications networks (e.g., European Union's (EU) Directive on Security of Network and Information Systems[20]).

On the device side, not long ago, as put bluntly by a security expert, poor security practices had become "so endemic and so deeply entrenched throughout the world and its supply chains" that the prospect of reversing course seemed nearly impossible (Rogers, 2021). Yet, the last few of years can be regarded as the reckoning from the private sector's failings to prioritise and address in a more systematic way the security risks of devices and software[21]. Mandatory rules in this area are still emerging but the calls to make manufacturers liable for security vulnerabilities is a notable trend, as seen with the EU's proposal for the Cyber Resilience Act[22]. Even countries which had long favoured non-mandatory approaches and market's 'self-regulatory' power, such as the US, are now espousing regulatory routes[23].

As part of these new measures, policymakers are increasingly leaning on third party assessments and certification schemes for industry, namely manufacturers, to demonstrate a level of cybersecurity assurance and prove their products are compliant with new regulations. Certification can be useful in supporting regulators in their compliance-monitoring role, but does not, on its own, guarantee robust levels of security. Indeed, certification obtained based on information provided at one point in time cannot account for the dynamic and ever-changing

---

[13] Such as the recent guidance endorsed by seven countries: the US, Australia, Canada, the United Kingdom, Germany, the Netherlands and New Zealand. See Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by Design and -Default, 2023.
[14] Telecommunications security and integrity regulation, 2021.
[15] Telecommunications Cybersecurity Code of Practice
[16] Electronic Communications (Security Measures) Regulations and Telecommunications Security Code of Practice , 2022.
[17] Loi n° 2019-810 du 1er août 2019 visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles
[18] Telecommunications Sector Security Reforms (TSSR) , 2022.
[19] 'Trusted Telecoms Portal' under the National Security Directive on Telecommunication Sector , 2021.
[20] See European Commission's New stronger rules start to apply for the cyber and physical resilience of critical entities and networks, 2023.
[21] For instance, the Cybersecurity Tech Accords is an industry agreement launched in 2018 in which signatories pledge to protect users and customers, including through the development of products and services that prioritise security, privacy, integrity and reliability. See also the 2022 OECD Recommendation of the Council on the Digital Security of Products and Services calling for the improvement of digital security of products and services and a "duty of care" for suppliers to integrate digital security at every stage of the product's lifecycle.
[22] European Commission's Cyber Resilience Act Proposal, 2021.
[23] The US' recent National Cybersecurity Strategy clearly marks the country's intention to propose new cybersecurity regulations, see the National Cybersecurity Strategy Implementation Plan, 2023.

threat landscape, which is especially true when assessing software-based products given their millions of lines of code and frequency of updates (Information Technology Industry Council, 2020).

Nevertheless, the key takeaway is that governments and other relevant agencies have sent a strong signal to the industry: cybersecurity should no longer be an after-thought. Instead, networks and devices should be "secure-by-design". The idea of building security principles into technologies at the outset of product design and development is an important step forward but it should not be reduced to a tick box exercise. A comprehensive approach to cybersecurity is multi-faceted, part of an iterative process, and crucially, it is as much a government objective as it should be for the industry.

The stakes are high: new compliance requirements aside, industry gains in investing in cybersecurity

Remarks about how policymakers have failed to keep pace with the fast changing technological world are cliché but not without reason – the legislative process is often protracted [24]. As legislation gets implemented, and the threat of exorbitant fines for non-compliance materialises, the market incentives should drive industry to invest in cybersecurity. As the previous section alludes to, suffering from a cyber-attack and data breach is no longer a question of "if" but "when". While investing in cybersecurity is expected to increase a company's spending, this cost significantly outweighs the financial and reputational losses in the aftermath of a cyber-attack (Keman Huang, 2023). In this regard, a recent global survey reported that business and cyber leaders think effective enforcement of regulatory requirements is helpful in raising the quality of cybersecurity across their sector and their supply chains, not least because it helps signpost at board-level discussions the need to invest in cyber resources (World Economic Forum (WEF), 2023).

Industry, and more specifically manufacturers and developers of software products, are usually best placed to remediate security flaws identified in their systems and devices. As mentioned above, applying a "secure-by-design" approach does not guarantee a system will be immune of vulnerabilities, but identifying and fixing them are crucial to preventing these from being exploited by malicious actors [25]. In fact, companies are setting up Coordinated Vulnerability Disclosures (CVD) programmes designed to provide a mechanism for the security research community to safely disclose security flaws which can then be addressed and communicated to the public. This structured process helps companies improve the security of technologies overall[26].

---

[24] Having legislation and regulations in different countries raises the risk of having potentially diverging and/or contradictory compliance requirements. The technology industry operates across borders and multiple jurisdictions, predominantly at a global scale. Whilst not addressed in this essay due to scope, policymakers and regulators should ensure they consult with industry, as well as other stakeholders, throughout the process of setting cybersecurity regulatory frameworks and not in isolation of the international context to minimise unwarranted divergences. E.g., OECD's International Regulatory Co-operation, 2021.

[25] A recent study found a strong correlation between poor "patching cadence" for vulnerabilities and the likelihood of experiencing a cyber-attack. See Marsh McLennan Cyber Risk Analytics Center analysis of BitSight data, a security rating company, 2022.

[26] Worth mentioning that governments are also setting up CVD programmes at the national level, usually with the involvement of the national Computer Emergency Response Team or national cyber agency, to promote the process as good practice and coordinate vulnerabilities affecting governmental institutions

Moreover, one cannot underestimate the role technology standards play in securing networks and products. The fruit of a collaborative effort, a standard generally consists of a document, usually established by a consensus and approved by a recognised body, that provides guidance on a recognised way of doing something (International Organisation for Standardisation (ISO), n.d.). International and regional standards development organisations are important forums where the technical community, usually practitioners from industry, come together and see standards adopted and embedded in products and networks. A principal motivator for standardisation had been enabling interoperability of technologies between different countries and regions. Nowadays, good security practices are also driving industry to standardise guidance in this field, as seen with the first global standard for the security of Internet of Things consumer devices[27].

Beyond governments and industry: cybersecurity is a shared individual and collective responsibility

It has been said that security is only as strong as the weakest link or component of a system (DeNardis, 2020). While improving security of networks and devices on the market is key, promoting similar ambitions in the systems we use internally and amongst the population go hand-in-hand.

Organisations are adopting internal risk management frameworks to effectively reduce the risk of unauthorised access and misuse of data. Within the series of well-known ISO 27000 cybersecurity standards, ISO/International Electrotechnical Commission (IEC) 27001[28] outlines the practices an organisation can implement to protect the confidentiality, integrity and availability of its information and assets[29]. Similarly, the zero-trust architecture, which assumes that no connection or device is safe and needs to be validated within a network, has become a popular security model for organisations globally (National Institute of Standards and Technology (NIST), 2020). Indeed, in 2022, 55% of companies surveyed reported having in place a zero-trust architecture, up from 24% in 2021 (Okta, 2022). On the government side, there has been momentum for the adoption of this framework, namely in the US through President Biden's executive order which mandates the adoption of zero trust across federal agencies and its contractors[30]. Whilst governments and industry have been in focus, it is important to stress that cyber-attacks are far reaching, affecting Non-Governmental Organisations (NGOs) and educational institutions alike[31]. Supporting initiatives geared towards building their capacity to withstand cyber-attacks are helping to foster a holistic sectoral approach to cybersecurity[32].

---

or organisations related to critical infrastructure. E.g., ENISA's Coordinated Vulnerable Disclosure Policies in the EU, 2022.

[27] The European Telecommunications Standards Institute (ETSI) EN 303 645: Cyber Security for Consumer Internet of Things: Baseline Requirements, 2020.

[28] ISO/IEC 27001 - Information Security Management (ISMS).

[29] These include but are not limited to using multi-factor authentication, access controls and encryption.

[30] The White House's Executive Order on Improving the Nation's Cybersecurity, 2021.

[31] According to Microsoft's Digital Report 2022, the NGOs/Think tanks and the education sectors are the second and third most targeted sectors globally by Nation State actors. These types of entities are particularly vulnerable given they usually have limited resources, which can impact their ability to invest in cybersecurity and thereby, be perceived by cyber criminals as easier targets to compromise their systems and data. These types of entities also tend to hold large amounts of personal and sensitive information about people they interact with and serve which can be exploited for financial gains.

[32] E.g. CyberPeace Institute Humanitarian Cybersecurity Center and NetHope's Digital Protection Programme.

Finally, the way an organisation instils and embraces a culture of cybersecurity is fundamental. With the evolving threat landscape, the risk of cyber-attacks is high and while technical security controls can help, pursuing "soft controls" such as cyber hygiene, meaning the proactive steps one can take to improve their security and privacy in the cyber domain, can go a long way. This is especially important considering a majority – between 55%-75% depending on the study – of cybersecurity incidents in the last few years are due to human error (Thales, 2023) (Verizon, 2023). Promoting an understanding of the cyber risks across the organisation and establishing proactive steps for personnel to report breaches are essential in protecting access to networks, devices and data. Beyond the organisational level, efforts in educating the population about the risks of cyber-attacks and communicating steps individuals can take to protect themselves should continue to be prioritised. Alongside running dedicated cybersecurity awareness campaigns, such as October's Cybersecurity Month[33], national agencies are now producing practical tips available for citizens [34][35]. As a longer-term measure, cyber hygiene and training are being integrated into school curriculums (WEF, 2020). Drawing a parallel with online safety can be useful in this regard: along with enacting legislation that regulates illegal content online, Australia has developed a national framework for online safety education and created toolkits for schools and universities to help students build an awareness of harms online as well as promote a sense of responsibility in using digital technologies [36]. This two-pronged model in legislating to safeguard online users' experiences whilst also educating the population, in this case younger users, sets a good precedent for incorporating cyber hygiene measures in similar digital literacy programmes within educational settings. Estonia is a noteworthy example: digital competence under the nation's curriculum describes the cybersecurity knowledge and skills young people should receive as part of their education[37].

Conclusion

We have come a long way since university student Robert Tappan Morris inadvertently launched one of the first high-profile cyber-attacks in 1988 leading the reporter covering the story at the time to write "They [computer security experts] said the attack would serve as a useful lesson that not enough attention was being paid to computer security" (Markoff, 1988) [38]. Thirty-five years on, cyber-attacks have become more prominent but at least, greater attention is being paid

[33] Observed globally to raise awareness about cybersecurity. Countries take the opportunity to disseminate campaigns for the general public offering practical tips about good practices, as seen in the United States, European Member States, Nigeria, South Africa and many more.
[34] Non-exhaustive list: United Kingdom's NCSC Cyber Aware Initiative, Belgium's Cyber Security Centre Stay Safe, Estonia's Be IT-Conscious and Singapore's Cybersecurity Agency GoSafeOnline. There are also demographic specific campaigns such as Singapore's Cyber Safe Seniors and Australia's Mighty Heroes campaign for 5 to 8 years old which includes a segment on protecting personal information.
[35] Such initiatives are not only being promoted by national agencies, NGOs are also taking on this important mission, e.g. Africa Cybersecurity & Digital Rights Organisation (ACDRO).
[36] See e-Safety Commissioner's Best Practice Framework for Online Safety Education.
[37] See Estonia's National Cybersecurity Strategy 2019-2022. Further read: Cyber security education in Estonia: from kindergarten to NATO Cyber Defence Centre, 2022.
[38] The Morris Worm was programmed to exploit vulnerabilities in a type of operating system and resulted in drastically slowing down, and even crashing, some computers connected to the then Internet in the US. The incident received high media attention and is considered to be the precursor to what is known today as a distributed denial of service (DDoS) attack: a type of cyber-attack that tries to make a website or network resource unavailable by flooding it with malicious traffic so that normal traffic cannot reach its intended destination.

to cybersecurity. While we know that technology can never be 100 percent secure, I propose in this essay that a concerted effort from multiple players can help mitigate the risk of cyber-attacks and protect our data from breaches. Governments have a role in setting higher cybersecurity requirements for technologies we use and rely on, and the industry is having to comply with these new requirements and invest in direct measures to improve the security levels of technologies. However, cybersecurity is not limited to improving the security of networks and devices on the market nor solely a concern for governments and industry. Cybersecurity should be viewed as a holistic, shared and long-term responsibility. To illustrate this point, I highlighted how bringing internal measures to protect systems and data and ingraining a culture of cybersecurity at the organisational and individual level are steps that governments and industry are championing, but ultimately, we should collectively work towards ensuring that cybersecurity is at the forefront, and not on the edge, of our society and economy.

List of citations

Center for Strategic and International Studies. (n.d.). *Significant Cyber Incidents Since 2006*. Retrieved April 2023, from Center for Strategic and International Studies: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-04/230404_Significant_Cyber_Events.pdf?VersionId=3UxjuqXLPluSCUtSXhGM1ZecgewJ4wPI

Cisco. (2020, March 9). *Cisco Annual Internet Report (2018–2023)*. Retrieved from Cisco: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

DeNardis, L. (2020). *The Internet in Everything: Freedom and Security in a World with No Off Switch.* Yale University Press.

European Union Agency for Cybersecurity (ENISA). (2022, November 3). *Enisa Threat Landscape 2022.* Retrieved from ENISA: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Information Technology Industry Council. (2020, September). Policy Principles for Cybersecurity Certification. Retrieved from https://www.itic.org/policy/ITI_PolicyPrinciplesforCybersecurityCertification_Final.pdf

International Organisation for Standardisation (ISO). (n.d.). *What are standards and how do they help?* Retrieved from ISO: https://www.iso.org/sites/ConsumersStandards/1_standards.html#section1_1

International Telecommunications Union. (2021, June). *Global Cybersecurity Index 2020.* Retrieved from ITU: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

Keman Huang, X. W. (2023, May 4). *The Devastating Business Impacts of a Cyber Breach*. Retrieved from Havard Business Review: https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach

Koetsier, J. (2022, August 31). Smart Home: Apple Is The Fastest-Growing Connected Device Company. *Forbes*. Retrieved April 2023, from https://www.forbes.com/sites/johnkoetsier/2022/08/31/smart-home-apple-is-the-fastest-growing-connected-device-company/

Markoff, J. (1988, November 5). Author of Computer 'Virus' Is Son Of N.S.A. Expert on Data Security. *New York Times*, p. 1. Retrieved from https://www.nytimes.com/1988/11/05/us/author-of-computer-virus-is-son-of-nsa-expert-on-data-security.html

Meltware and We Are Social. (2023, January 26). *2023 Global Digital Report.* Retrieved April 2023, from Meltware: https://www.meltwater.com/en/global-digital-trends?

National Cyber Security Centre (NCSC). (n.d.). *What is cyber security?* Retrieved April 2023, from NCSC.gov.uk: https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security

National Institute of Standards and Technology (NIST). (2020, August). Zero Trust Architecture. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Norton. (2021, January 18). *Privacy vs. security: What's the difference?* Retrieved from Norton: https://us.norton.com/blog/privacy/privacy-vs-security-whats-the-difference

Okta. (2022, September). *The State of Zero Trust Security 2022.* Retrieved from Okta: https://www.okta.com/resources/whitepaper-the-state-of-zero-trust-security-2022/thankyou/

Organisation for Economic Co-operation and Development (OECD). (Forthcoming). *Enhancing the security of communication infrastructure.*

Rogers, D. (2021, November 24). *The Long Road to a Law on Product Security in the UK*. Retrieved from https://mobilephonesecurity.org/.

Standard and Poor. (2023, April 6). *5G tracker: 94 markets worldwide have commercial 5G services*. Retrieved May 2023, from S&P Market Intelligence: https://www.spglobal.com/marketintelligence/en/news-insights/research/5g-tracker-94-markets-worldwide-have-commercial-5g-services

Thales. (2023, April 18). *2023 Thales Data Threat Repor.* Retrieved from https://cpl.thalesgroup.com/data-threat-report

The International Association of Privacy Professionals . (2023, March 23). *Privacy and Consumer Trust.* Retrieved April 2023, from IAPP: https://iapp.org/news/a/most-consumers-want-data-privacy-and-will-act-to-defend-it/

Verizon. (2023, June 6). *2023 Data Breach Investigations Report.* Retrieved from https://www.verizon.com/business/resources/reports/dbir/

World Economic Forum (WEF). (2020, December 17). *After reading, writing and arithmetic, the 4th 'r' of literacy is cyber-risk.* Retrieved from https://www.weforum.org/agenda/2020/12/cyber-risk-cyber-security-education

World Economic Forum (WEF). (2023, January). *Global Security Outlook Report.* Retrieved from https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf