IIC FUTURE LEADERS' COMPETITION 2023

Policy essay on *Cybersecurity on the Edge?*

Table of Contents

Abstract

Internet-connected 'always on' systems and devices present one of the greatest privacy and cyber security challenge to nations, their governments, economies, and societies. The fast-paced development of new digital technologies and the growing number of smart IoT devices amplify this challenge.

The success or failure to address cyber security and privacy challenges in this context will have implications for our trust in the internet. Therefore, it is vital for policymakers to address those challenges effectively and in a timely manner.

Based on our secondary research and analysis of literature and governments' policy initiatives, we identify and recommend 'tools' that could lead to effective cyber threat mitigation.

We conclude that not one single actor or solution is able to combat cyber security threats and privacy risks. Instead, a holistic whole-of-nation approach must be adopted that involves all stakeholders and focuses on building cyber resilience across all sectors, industries, and societal groups.

Cyber security and privacy in a digital world

The number of smart Internet of Things (IoT)[1] devices connected to the Internet already exceeds the number of people using the internet. Globally, the number of such devices is forecast to grow to more than 29 billion by 2030 (from 9.7 billion in 2020).[2] Additionally, a wealth of new digital technologies such as blockchain, virtual reality (VR), augmented reality (AR), artificial intelligence (AI)[3], 5G and quantum computing, impact how we communicate, work, and transact.

As these technologies and devices promise to dramatically improve the speed, scalability and efficiency of interconnectivity, they pose new cyber security and privacy threats by collecting increasingly granular data points. For instance, AI-enabled VR goggles collect and produce a myriad of biometric information, which is the key to our identity. The eye-tracking of our gaze direction and pupil reactivity contains information about our gender, age, ethnicity, body weight, medical condition, and emotional state. This wealth of intimate data points poses significant privacy risks and makes us vulnerable to cyber security breaches.

[1] IoT refers to the network of physical devices embedded with sensors, software, and network connectivity, which enables these objects to connect and exchange data over the Internet. These devices, often referred to as 'smart' devices, can be remotely controlled and are able to interact with each other autonomously. The IoT has applications across various sectors, including consumer, industrial, agricultural, and medical contexts, among others.

[2] Statista (2022): Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030, November 2022, available at: IoT connected devices worldwide 2019-2030 | Statista (accessed on 24 May 2023).

[3] Including large language models (LLMs) like generative AI.

The problem is that like the internet, many of those technologies and smart devices were not built with cyber security and privacy in mind.[4] In fact, cyber security and privacy were – and often still are – secondary considerations.[5] As digital technologies and smart devices become more diffuse and less visible because they are embedded in physical infrastructures (e.g., transportation, hospitals), consumer goods (e.g., smart fridges, TVs, goggles) and systems (e.g., payment systems), the implications of these developments become more concealed, and cyber security and privacy issues become more ominous.

To add to the complexity, many organisations that do not view themselves as traditional internet companies or tech firms are now transitioning into this realm, embedding both digital and material components.[6] For example, financial services firms like WeBank and Sberbank are increasingly transitioning to data-driven, technology-enabled online platforms.[7] Sports equipment manufacturers such as Under Armour produce digitally connected smart shoes.[8] Automobile companies like Tesla work on autonomous vehicles that embed communications technology.[9] Many of these firms have historically less or no experience with cyber security and privacy.[10]

It is a sobering thought that approximately half of the world's population is now part of this interconnected digital environment, and therefore vulnerable to breaches – knowingly and unknowingly. An even more sobering thought is that not only our smart consumer goods but also technologies and devices underpinning critical infrastructure such as power generation, water distribution, hospitals, and road- and air-traffic control systems are exposed to security vulnerabilities. As we are seeing an escalation of cyber warfare due to geopolitical disagreements, securing digitally connected critical infrastructure assets becomes more important than ever before.

Considering these developments, policymakers are under pressure to reconceptualise existing regulations and policies to account for the implications of these technological advancements.

Cyber breach mitigation: some recommendations for policymakers

In the race to combat cyber security risks, governments feel a need to 'do something'.[11] Globally, several policy and regulatory initiatives at the intersection of cyber security and privacy are under development or have been finalised.[12] Some of those governments

[4] Tusikov, N. (2019), pp. 59-60
[5] Cameron, L. (2023)
[6] Zuboff, Shoshanna (2019)
[7] Browne, R. (2019)
[8] Miller, M. (2021)
[9] Tesla (2023)
[10] Denardis, L. (2020), pp. 44-48
[11] Madnick, S. (2022)
[12] They include Australia's 2023-2030 National Cyber Security Strategy, China's and Russia's data localisation requirements, India's CERT-In incident reporting requirements, and the European Union's Cyber Security Act.

seem to focus on the number and complexity of (additional) regulations rather than proposing fit-for-purpose 'tools' in a timely manner.

Our analysis shows that notwithstanding above-outlined challenges, the dynamic nature of the digital ecosystem also presents ample opportunities to make the online world more secure. In the following sections, we explore some tools and assess how they could contribute to more robust and effective cyber breach mitigation with focus on privacy.

Security-by-design from the onset

The competitive pressure to bring digital technologies and smart devices quickly to market at the cheapest possible price has often diminished the potential for thoughtful long-term security and privacy design from product inception. Security experts claim that up to 60 per cent of IoT devices on the global market are completely unsecure.[13] It is therefore unsurprising that those devices are occasionally referred to as 'zombie devices' that can easily be subverted to assist in cyber-attacks.

Considering the wealth of personal and sensitive information shared via smart devices and technologies, such security vulnerabilities pose real threats to our privacy and national security. Privacy and security cannot be afterthoughts - they must be built in from the outset and continuously managed in all phases of the product and system lifecycle.

In April 2023, the US Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and cyber security authorities of Australia, Canada, United Kingdom, Germany, Netherlands, and New Zealand released their joint guidance on *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default*. It urges manufacturers to build products that are secure-by-design and -default. However, whilst such guidance sounds good in theory and is supported by several internationally recognised frameworks and standards[14], the reality is that building in security from the outset is difficult.

Systems and devices are rarely designed by one manufacturer from scratch. They contain components made in various countries and are designed in accordance with different standards – if any standards at all. They may draw from code already written, whether open source or otherwise, and be built on existing operating systems. This makes building security-by-design into products and systems from the beginning increasingly difficult.

Further, some security-by-design mechanisms like upgradability bring their own cyber security risks.[15] The upgrade process, such as downloading a patch automatically and wirelessly, presents an opportunity for a malicious actor to implant malware or initiate

[13] Burton, T. (2023)

[14] E.g., National Institute of Standards and Technology (NIST) Cyber-Physical Framework, ESTI EN 303 645 (Cyber Security for Consumer Internet of Things), ISO 31700 (Consumer protection — Privacy by design for consumer goods and services)

[15] Internet Society (2020), p. 15

Distributed Denial-of-Service (DDoS) attacks. The upgrading process itself may therefore require several dimensions of extra security checks.

Even though governments should demand from manufacturers and vendors to take more responsibility and accountability for the security of their products and systems, the execution is not that easy. In essence, security-by-design is necessary but not, by itself, sufficient.[16] Below, we discuss Cyber Security Labelling Schemes (CLS), seemingly a gradual extension of and/or complementary tool to security-by-design principles.

Cyber security labelling schemes

A recent policy consideration is CLS to improve the security of smart IoT devices while protecting consumers' data privacy. The Cyber Security Agency of Singapore[17] has launched a CLS for consumer smart devices, as part of the agency's efforts to raise overall cyber resilience of the nation. The CLS is the first of its kind in the Asia-Pacific region. Germany has also introduced the so-called *IT Security Label* for consumer protection.

CLS could help consumers to objectively compare smart devices and make more conscious purchases based on security claims, thus enhancing cyber hygiene across the IoT ecosystem and broader society. Labels indicating the cyber security level would be particularly helpful for consumers purchasing products from manufacturers that are not traditional tech companies and therefore lack expertise in the cyber and privacy domain.

Opponents of such schemes have argued that manufacturers and vendors would have to absorb additional compliance costs, which are likely to be passed on to end-consumers. On the other hand, proponents claim that CLS could potentially incentivise manufacturers to ensure their products are secure, thereby causing a 'healthy' competition in the market for the most secure products and systems.

Globally, there is no consensus on whether CLS should be voluntary or mandated. Most likely, IoT will continue to be a marketplace where the compromises between price and quality will continue to push consumers on the side of cheap rather than secure products. Against this background and in consideration of the lack of internationally harmonised standards, a mandate is necessary in the medium to long term.

Whether mandated or not, a CLS requires a multi-stakeholder approach involving regulators, policymakers, manufacturers, vendors, academia, and civil society in the ongoing development and updates of such schemes.

National digital identity systems

As we are moving from Web 2.0 (the internet as we know it) to Web 3.0, a more open, immersive and personalised version of the internet built on new digital technologies such as blockchain, the role of our digital identities grows in importance. Our digital identities

[16] Crabtree, A. et al. (2021), pp. 60-63

[17] For more information, see https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme (accessed on 30 June 2023)

do not only represent who we are in the online worlds, they are integral to the development and functioning of our digital economies and societies.

This requires a rethink by policymakers of how to secure our identities online. Continued large-scale data breaches[18] show that authenticating individuals through passwords cannot reliably assure identity. That is why several jurisdictions including the European Union[19], Australia[20] and the United States[21] have started developing national digital identity schemes to protect citizens' personal information from being misused and stolen.

Some of the data held by those national digital identities and their underlying digital wallets is particularly sensitive (e.g., passport number, date of birth). Hence, governments should prioritise taking a minimalist approach to data collection and retention. Once governments verified our identity and the digital identity is established, source documents containing sensitive information should not be retained by default.

While this constitutes a radical shift from current data handling by most governments, it is one that is indispensable for our privacy and security – as well as our trust in the digital economy. The less data is retained, the less incentivised malicious actors are to execute attacks.

With respect to breach mitigation and privacy, governments should explore and consider Privacy Enhancing Technologies (PETs) as part of their digital identity strategy. PETs are digital solutions that allow information to be collected, processed, analysed, and shared while protecting data privacy.[22] While not fundamentally new, these digital technologies and techniques provide novel approaches to anonymisation, pseudonymisation, confidentiality, data minimisation and protection while in use.[23]

The EU, for example, recognises blockchain's features of encryption and Zero-Knowledge Proof (ZKP)[24] as potential privacy-enhancing solution supporting European digital identity wallets.

[18] For example, the Medicare (health insurance provider) breach in 2022 affected 9.7 million Australians and the Twitter cyber-attack affecting more than 400 million users worldwide.
[19] The European Commission is finalising its *European Digital Identity* including the *Electronic Identification and Trust Services (eIDAS) Regulation*.
[20] Australia is working on its *Trusted Digital Identity Framework (TDIF)* and *National Strategy for Identity Resilience*.
[21] The *Improving Digital Identity Act* was passed by the US Senate Homeland Security and Governmental Affairs Committee in April 2023.
[22] OECD (2023), pp. 10-13.
[23] Dieye, M. et al. (2023), pp. 49449-49453.
[24] ZKP mechanisms as deployed by public blockchains and their smart contract function, can enhance data privacy and security by answering the simple question of whether something is true or false without revealing any additional information. ZKP hides the underlying sensitive data such as the date of birth while answering whether someone has reached mature age. Thus, ZKP could help shift the paradigm from requiring users to reveal their sensitive data to allow others to verify certain claims.

Cyber intelligence sharing at speed and scale

As cyber-attacks become more sophisticated and wide-reaching, there is a growing need for speed and scale of threat intelligence sharing among government agencies and between governments and private sector entities.

Sharing threat intelligence and 'learning from others' becomes a crucial exercise in developing mitigation strategies and building cyber resilience collectively. Keeping cyber threat insights in information siloes hampers private and public sector efforts to combat cybercrime. In fact, not sharing threat intelligence at speed and with relevant organisations (such as critical infrastructure operators) and agencies (such as defence ministries) can have disastrous consequences.

For such reasons, governments must find ways to optimise information sharing efforts. Public-private partnerships in form of industry-led Information Sharing and Analysis Centres (ISACs) have the capabilities to overcome previously mentioned challenges. ISACs allow for two-way sharing of information between the private and the public sector about root causes, incidents and threats, as well as sharing experience, knowledge and analysis.[25] They gain rich sectoral insights that governments cannot achieve alone.

ISACs contrast with merely reporting breach information to satisfy compliance and/or regulatory requirements. In fact, they help aggregate industry-sourced insights into actionable intelligence that other organisations can leverage to develop cyber breach mitigation tactics and governments can use to build stronger cyber defence mechanisms, policies and regulations.

ISACs could represent compelling 'next-generation' threat mitigation, management, and prevention initiatives.

Adopting a whole-of-nation approach towards cyber resilience

The responsibility to keep nations, their economies, and societies secure while preserving their privacy does not lie with one stakeholder group. Cyber security must be considered as a collective responsibility that requires 'all-hands-on-deck' actions by *all* stakeholders. This requires a cultural shift from attempting to prevent all cyber-attacks – which becomes increasingly unachievable, if not impossible – towards building stronger cyber resilience across the economy and society to limit the impacts of inevitable breaches.

To operationalise a holistic whole-of-nation approach towards cyber resilience, governments must start by leading through better coordinated multistakeholder engagements to gain comprehensive understanding of different stakeholders' needs. Addressing stakeholders' needs, governments should start by uplifting cyber security awareness, skills and education across businesses and societal groups through several initiatives.

[25] ENISA (2023)

Governments should encourage and incentivise large tech firms to support businesses, particularly small and medium-sized businesses (SMEs) in developing and adopting well-defined and well-rehearsed recovery strategies. With attackers honing their craft to inflict maximum damage, businesses need to build resilience to ensure that an attack is a relatively minor inconvenience rather than a catastrophic incident.

From a workforce perspective, government should consider moving away from 'quick fix' approaches such as issuing 'emergency visas' to attract cyber security professionals from overseas, towards building a stronger cyber security workforce domestically.

As opposed to cyber security being a standalone discipline in tertiary education, governments should integrate cyber security throughout the broader education life cycle starting at schools or earlier. Cross-disciplinary cyber security education would support broader cyber resilience and hygiene and contribute to a healthier pipeline of the cyber-proficient workforce of the future. This is particularly important in developing countries, where a lack of resources and expertise, and a 'brain-drain' to more industrialised countries can cause long-term vulnerabilities.

Individuals across all generations deploy new technologies and smart devices, and therefore need to know how to protect themselves. Large-scale, national TV, radio and online campaigns are required to educate individuals of all ages and backgrounds about steps to take to reduce certain risks. When we all have a common understanding of the threat environment and take precautionary action – at home, in the workplace, and in our communities – using digital technologies and smart devices becomes a more secure experience for everyone.

Conclusion

The lack of adequate cyber security and privacy in the digital ecosystem affects everyone. Step change is needed to embed cyber awareness and incentives into everyday conversations, to make it an integral part of the national psyche.

While none of the policy tools outlined in this essay are in themselves sufficient to address cyber security and privacy concerns in the digital world, when combined, they have the capacity to lead to effective cyber risk mitigation.

However, we also note that the constantly evolving nature of cyber threats means that mitigating cyber threats and increasing resilience is not a one-off exercise, but a continuous effort that requires vigilance, adaptation, and investment from everyone.

Malicious actors will only stand no chance if *all* stakeholders take *joint* responsibility. Adopting a whole-of-nation approach, all stakeholders must be involved in creating a more secure and privacy-preserving digital environment.

Abstract: 150 words

Total (excl. footnotes and bibliography): 2876 words

Bibliography

Australian Department of Home Affairs (2023): 2023-2030 Australian Cyber Security Strategy – Discussion Paper, March 2023, available at: 2023-2030 Australian Cyber Security Strategy (homeaffairs.gov.au) (accessed on 16 June 2023).

Browne, R. (2019): Banks must behave 'more like technology companies' to survive, finance execs say, *CNBC*, November 2019, available at: Banks must behave like tech companies to survive amid fintech threat (cnbc.com) (accessed on 26 June 2023).

Burton, T. (2023): Industry calls for quick embrace of mandatory smart devices code, *Australian Financial Review*, January 2023, available at: Industry calls for quick embrace of mandatory smart devices code (afr.com) (accessed on 14 June 2023).

Cameron, L. (2023): Keynote address – Cyber 2023, Cyber security and the global economy, Chatham House conference, hybrid event, 14 June 2023, London.

Crabtree, A. Haddadi, H., Mortier, R. (2021): Privacy by Design for the Internet of Things - Building accountability and security, The Institution of Engineering and Technology, London.

Denardis, L. (2020): The Internet In Everything: Freedom And Security In A World With No Off Switch, New Haven & London, London.

Dieye, M. et al. (2023): A Self-Sovereign Identity Based on Zero-Knowledge Proof and Blockchain, *IEEE*, 11(1), pp. 49445-49455.

ENISA (2023): Information Sharing and Analysis Centers (ISACs), available at: Information Sharing and Analysis Centers (ISACs) — ENISA (europa.eu) (accessed on 29 June 2023).

Internet Society (2020): Policy Toolkit on IoT Security and Privacy, August 2020, pp. 1-35, available at: IoTtoolkit-Final August 2020 (internetsociety.org) (accessed on 19 June 2023).

Madnick, S. (2022): New Cybersecurity Regulations Are Coming. Here's How to Prepare, *Harvard Business Review*, August 2022, available at: New Cybersecurity Regulations Are Coming. Here's How to Prepare. (hbr.org) (accessed on 27 June 2023).

Miller, M. (2021): Running with Under Armour connected shoes: HOVR and Velociti propel my All Out Mile attempt, *ZD NET*, November 2021, available at: https://www.zdnet.com/article/running-with-under-armour-connected-shoes-hovr-and-velociti-propel-my-all-out-mile-attempt/ (accessed on 26 June 2023).

OECD (2023): Emerging Privacy Enhancing Technologies – Current Regulatory and Policy Approaches, *OECD Digital Economy Papers*, March 2023, pp. 1-51.

Statista (2022): Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030, November 2022, available at: IoT connected devices worldwide 2019-2030 | Statista (accessed on 24 May 2023).

Tesla (2023): Autopilot and Full Self-Driving Capability, available at: Autopilot and Full Self-Driving Capability | Tesla Support Australia (accessed on 27 June 2023).

Tusikov, N. (2019): Regulation through "bricking": private ordering int the "Internet of Things", *Internet Policy Review,* 8(2), pp. 56-87.

Zuboff, Shoshanna (2019): The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, Public Affairs, New York.