Securing the Edge: Policy Perspectives on Cybersecurity and Privacy

Abstract

In today's rapidly changing digital world, ensuring robust cybersecurity and protecting privacy are of utmost importance. This essay explores the role of policy development in achieving these objectives, with a particular focus on the concept of "security by design." It highlights the need to integrate security and privacy considerations right from the start of technology development. Agile policy responses, international cooperation, and shared responsibilities among governments, developers, organisations, and individuals are identified as vital elements for mitigating breaches, safeguarding privacy, and maintaining a secure digital environment.

Securing the Edge: Policy Perspectives on Cybersecurity and Privacy

As online technologies evolve, robust cybersecurity becomes crucial. In today's rapidly evolving digital landscape, businesses face intense competition as they strive to leverage online technologies while ensuring security and privacy (Quach et al, 2022). Staying ahead in the market requires an understanding of how evolving technologies and interconnected networks impact the competitive landscape.

This essay explores policy development for addressing emerging threats in interconnected networks. We focus on challenges from edge devices and IoT (Internet of Things), the feasibility of "security by design," and preventing data misuse while prioritising privacy. The proliferation of edge devices presents unique challenges, requiring tailored security measures. Policy agility is vital in responding to evolving cybersecurity risks and preventing data misuse. Privacy protection is essential, balancing security with individual rights. Strong data protection measures like encryption and access controls mitigate breaches. Privacy-preserving techniques, such as data minimisation, safeguard privacy. Shared responsibility among governments, technology developers, organisations, and individuals is crucial in managing security and privacy challenges for a secure digital environment.

Policy Development for Security

While developing policy for cybersecurity, we also need to consider data protection and privacy. This ensures people's personal information such as their name, address, financials, online activities, and more are safeguarded from misuse. It protects people's rights to privacy and helps prevent identity theft and fraud.

Data protection and privacy are also important for building trust (Richards & Hartzog, 2020). Customers, citizens, or users can become confident that their information is protected. This can strengthen the image of an entity or government. It can help incline people to stick with a brand or become loyal to a government.

Aside from the benefits of maintaining data protection, many countries also have laws making it mandatory to have safeguards in place. For example, the Australian government's *Privacy Act 1988*[1] regulates how personal information is managed. The European Union also overseas data protection and privacy through the *General Data Protection Regulation* (GDPR)[2]*.* The set of rules mandate personal information that can be used to identify someone such as their name or address must be protected. The GDPR also requires organisations to take measures to protect data from unauthorised access and misuse. Examples of this can include encryption and multi-factor authentication. All of this shows how cybersecurity is inherently linked to data protection and privacy and must be reflected in policy.

To gain a competitive edge, businesses must develop policies that encompass comprehensive cybersecurity measures (Kosutic & Pigni, 2022). The market competition drives the need for strong security practices, as breaches and data misuse can have a significant impact on a company's reputation and market position (Makridis, 2021).

Some may argue that comprehensive policies and regulations are overly restrictive and impede innovation and technological advancements. They contend that a more flexible approach is needed, allowing market forces to drive security practices and innovation. They believe that businesses should have more freedom to develop technology without being overly burdened by strict regulations.

However, comprehensive policies and regulations are necessary to ensure consistent and effective security practices (Hsu et al., 2015). By establishing clear guidelines and standards, regulations provide a framework for responsible innovation that considers the evolving cybersecurity landscape. Balancing flexibility with security measures ensures that

[1] Privacy Act 1988 (legislation.gov.au)
[2] General Data Protection Regulation (GDPR) – Official Legal Text (gdpr-info.eu)

technological advancements are achieved without compromising the safety and privacy of individuals and organisations.

Edge Devices and the Internet of Things

Edge devices like smart phones and smart watches are examples of the IoT. These devices are all connected to the internet and allow communication between each other. But the connections between these devices and the internet can make it harder to keep things secure, as there are more entry points for breaches or something to go wrong. Edge devices come in different shapes and sizes, so it is important to ensure fitting security measures for each type of device. The measures should consider unique features and their scalability and size (Lu & Da Xu, 2018).

These devices and the IoT are examples of how as technology advances, cybersecurity becomes more difficult to maintain. Therefore, policies need to be made and change to address new threats as they arise. This includes addressing things like smart devices to ensure their specific security challenges are considered. Keeping policy adaptive and not confined to one type of scenario helps entities or governments a better chance of keeping data secure.

Security by Design

Security by design means considering security right from the beginning when creating something, for example a website or an app. It is important because it helps ensure that what we create is strong and protected from cyber threats. It also helps to keep our personal information private.

To achieve security by design, developers need to think about security measures from the beginning (Paananen et al., 2020). They should focus on things like making sure only authorised people can access the system, protecting information through encryption, and

controlling what people can do once they are inside.

An important security measure is encryption. It scrambles the information so that it is difficult for anyone who should not see it to understand what it says. Access controls are also important. They help determine what people can do once they are inside the system. This helps keep things organised and prevents unauthorised access to sensitive information.

In addition to security, privacy is also essential. It means keeping personal information safe and respecting people's rights to control their own data. Privacy-preserving techniques are used to ensure that personal information is protected.

One technique is data minimisation, which means only collecting the necessary information and not asking for more than what is needed. For example, filling out a form where they only ask for your name and age instead of asking for your address or phone number. Anonymisation is another technique. It involves hiding or removing information that can directly identify someone.

By considering security by design and using privacy-preserving techniques, we can create technology that is both strong and protects our personal information (Cavoukian & Dixon, 2013).

In the fiercely competitive market, businesses are investing in research and development to create secure edge devices and IoT solutions. Those who prioritise security by design can gain a competitive advantage by offering products and services that prioritise user privacy and protect against data breaches (Quach et al, 2022).

Critics may argue that achieving "security by design" in complex environments is impractical. The rapid pace of technological advancements and evolving threats make it difficult to

anticipate and address all security challenges from the outset. They may question the effectiveness of security measures designed for edge devices and IoT, suggesting that vulnerabilities may still exist despite security efforts.

While the evolving nature of technology presents challenges, integrating security measures from the initial stages of development remains crucial. By embedding security considerations into the design process, vulnerabilities can be identified and addressed proactively. While no system is entirely immune to threats, “security by design” significantly reduces the risk of breaches and strengthens overall cybersecurity (Pfleeger & Caputo, 2012). Tailoring security measures to the unique features and interconnectedness of edge devices and IoT is essential for safeguarding data and privacy in these complex environments.

Policy Agility in Data Misuse Prevention

The speed at which policy can prevent data misuse is a crucial concern in an ever-evolving digital landscape. Governments must adopt agile policy-making processes to respond quickly to emerging threats (Tashtoush et al., 2021). Dedicated teams, collaboration with experts, and flexible frameworks facilitate swift adaptation and effective cybersecurity measures.

Policy-making processes need to be agile, which means they need to be able to adapt and respond quickly to new challenges. Governments can achieve this by having dedicated teams that focus on cybersecurity and data protection. These teams work closely with experts who have the knowledge and skills to understand the ever-changing landscape of cyber threats. They collaborate to produce solutions and strategies to protect against data

misuse.

Having flexible frameworks is also important. This means that policies can be easily updated and changed as new threats emerge. Policies should be flexible enough to adapt to different situations and address new risks effectively.

Sceptics may express doubts about the agility of policy-making processes in responding to rapidly evolving cybersecurity threats. Traditional bureaucratic systems may be slow to adapt and lack the flexibility required to address emerging threats effectively. They may also question the ability of policymakers to stay up to date with the latest technological advancements and potential risks.

While bureaucratic processes can be perceived as slow, policy agility is crucial in combating evolving cybersecurity threats. Governments and regulatory bodies can establish dedicated teams and collaborate with experts to ensure the timely adaptation of policies. By adopting flexible frameworks and regularly reviewing and updating regulations, policymakers can effectively address emerging threats and stay abreast of the evolving technological landscape. The involvement of cybersecurity experts and stakeholders in the policy-making process contributes to greater responsiveness and adaptability to mitigate data misuse risks.

International Cooperation

Cybersecurity is a global concern, necessitating international collaboration. Sharing threat intelligence, harmonising standards, and establishing cooperative agreements enhance policy effectiveness in preventing cross-border data misuse (Chernenko et al., 2018).

One way they do this is by sharing threat intelligence. By working together, countries can identify and respond to threats more effectively. Another aspect is harmonising standards.

This means trying to have similar rules and guidelines across different countries to ensure consistency in cybersecurity practices.

Establishing cooperative agreements is also important. Countries can come together and make agreements to work jointly on cybersecurity issues. It's like forming a team with other countries to fight against cyber threats. By collaborating and sharing resources, they can be more effective in preventing cross-border data misuse.

In summary, policy agility in data misuse prevention means having processes that can quickly respond to emerging threats. This requires dedicated teams, collaboration with experts, and flexible frameworks. Additionally, international cooperation is crucial in addressing cybersecurity challenges by sharing threat intelligence, harmonising standards, and establishing cooperative agreements. By being agile and working together, we can better protect against data misuse and safeguard our digital world.

Mitigating Breaches in Cybersecurity

Mitigating breaches requires a comprehensive approach that prioritises privacy alongside robust cybersecurity measures (Algarni et al., 2021). Encryption, secure authentication, and access controls mitigate breaches and protect sensitive information. Privacy-enhancing technologies preserve individual privacy rights.

To mitigate breaches in cybersecurity, it's important to have strong data protection measures in place. These measures help keep sensitive information safe and protected.

Encryption is like putting information in a secret code that can only be understood by authorised people. It ensures that even if someone manages to access the information, they

will not be able to understand it without the key.

Secure authentication is about verifying the identity of users to ensure only authorised people can access certain information. It's like having a fingerprint or a passcode to unlock your phone. This helps prevent unauthorised access and reduces the risk of breaches.

Access controls help manage who can access certain information and what they can do with it. It's like having different levels of access in a building. Some people may have access to certain rooms while others can't enter those areas. Similarly, access controls restrict access to sensitive information and limit the actions that can be performed on that data.

Privacy-enhancing technologies are tools and practices that specifically focus on preserving individual privacy rights. They help ensure that personal information is protected and used in a way that respects privacy. For example, technologies that allow individuals to control how their data is shared, or techniques that minimise the amount of personal information collected, contribute to privacy protection.

Businesses are recognising the importance of privacy-enhancing technologies and transparent data handling practices in meeting customer expectations and gaining a competitive edge. Prioritising privacy protection not only builds customer trust but also sets businesses apart from their competitors in attracting and retaining customers.

Some stakeholders might prioritise cybersecurity measures over privacy concerns. Strong security measures are necessary to protect individuals and organisations from cyber threats, even if it means sacrificing certain privacy rights. They may assert that strict privacy regulations could hinder effective cybersecurity practices by limiting data collection and sharing, making it more challenging to identify and mitigate potential risks.

However, while cybersecurity is of utmost importance, privacy rights must also be safeguarded. Striking a balance between security and privacy is crucial for building trust and maintaining the integrity of online systems. Comprehensive data protection measures, including encryption and access controls, can mitigate breaches without compromising individuals' privacy. Effective cybersecurity practices can be implemented without infringing on privacy rights, ensuring that data is collected and shared responsibly while minimising the risks of unauthorised access and misuse.

Transparent Data Handling

Policies play a crucial role in mitigating breaches and protecting privacy. One important aspect is transparent data handling practices (Michael et al., 2019). This means that policies should require organisations to be open and clear about how they handle personal information. Individuals should be informed about how their data is collected, used, and shared.

Empowering individuals with control over their own data is also essential. Privacy settings and consent management give individuals the ability to decide how their personal information is used. It's like having control over what information you share with others. By giving individuals the power to manage their data, policies promote privacy protection and ensure that personal information is handled according to individual preferences.

In summary, mitigating breaches in cybersecurity requires a comprehensive approach that not only focuses on robust security measures but also prioritises privacy. Strong data protection measures like encryption, secure authentication, and access controls safeguard sensitive information. Privacy-enhancing technologies preserve individual privacy rights.

Policies that promote transparent data handling practices and empower individuals with control over their data contribute to privacy protection.

Shared Responsibility for Managing Security

Managing security and privacy challenges requires collaborative efforts and shared responsibility among separate groups of people involved (Shackelford, 2019).

Governments play a crucial role in developing and enforcing privacy and cybersecurity regulations. They create laws and rules that organisations must follow to protect individuals' privacy rights. These regulations establish legal frameworks that help ensure that personal information is handled responsibly and securely. Governments also promote compliance with these regulations by educating organisations and individuals about their rights and responsibilities. They provide oversight to monitor and enforce privacy and cybersecurity practices, making sure that organisations are accountable for protecting individuals' information.

Technology developers have a responsibility to create products and services that are secure and respect individuals' privacy. They need to adopt security by design principles, which means considering security from the very beginning when designing and developing technology. This involves building security measures into the products and services from the start. Developers also conduct testing to identify and fix any vulnerabilities or weaknesses that could be exploited by hackers or unauthorised users. Regular updates are provided to address emerging threats and ensure that the technology remains secure.

Organisations and businesses also have a responsibility to prioritise cybersecurity and privacy. They need to implement robust security measures to protect the data they collect and handle. This includes encrypting sensitive information and regularly updating security

systems. Organisations must conduct risk assessments to identify potential vulnerabilities and take steps to address them. They should also educate their employees about cybersecurity best practices to ensure everyone understands their role in protecting sensitive data. The importance of this can be seen in Wong et. al (2022), where policy awareness affected supply chain reactive capability. Compliance with privacy regulations is essential, and organisations must ensure that they handle personal information in accordance with the law and privacy rights.

Market forces drive businesses to take responsibility for cybersecurity and privacy. By prioritising these aspects, organisations can build a strong brand reputation and attract customers who value data security. This commitment to security and privacy sets them apart from competitors who overlook these factors.

Individuals have a role to play in maintaining security and privacy. Practising good cybersecurity hygiene is important, such as using strong passwords, being cautious of suspicious emails, and being mindful of what information they share online. By understanding the potential risks and taking steps to protect themselves, individuals contribute to the overall security and privacy ecosystem.

Critics may argue that individual responsibility in cybersecurity is overstated, placing an undue burden on individuals. They may suggest that stronger regulatory frameworks should be implemented, placing greater responsibility on organisations and technology developers to ensure security and privacy. They contend that a collective effort involving government, businesses, and technology experts is necessary to address security and privacy challenges effectively.

While collective efforts are essential, individual responsibility plays a role in maintaining cybersecurity. Individuals' awareness and adoption of good cybersecurity practices, such as

using strong passwords, updating software, and being mindful of data sharing, significantly contribute to overall security. Regulatory frameworks should establish a foundation for responsible practices, but individuals' active engagement is vital. Shared responsibility ensures that all stakeholders work together to mitigate security and privacy challenges effectively.

In today's ever-evolving digital landscape, policy development is crucial for robust cybersecurity and privacy protection. "Security by design" emphasises integrating security and privacy considerations from the beginning of creating technology. Swift policy responses, international cooperation, and shared responsibilities among governments, developers, organisations, and individuals are essential for mitigating breaches, protecting privacy, and ensuring a secure digital environment.

References

Algarni, A. M., Thayananthan, V., & Malaiya, Y. K. (2021). Quantitative assessment of cybersecurity risks for mitigating data breaches in business systems. *Applied Sciences, 11*(8), 3678.

Cavoukian, A., & Dixon, M. (2013). *Privacy and security by design: An enterprise architecture approach*. Information and Privacy Commissioner of Ontario, Canada.

Chernenko, E., Demidov, O., & Lukyanov, F. (2018). Increasing international cooperation in cybersecurity and adapting cyber norms. *Council on foreign relations*.

Hsu, J. S. C., Shih, S. P., Hung, Y. W., & Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information systems research, 26*(2), 282-300.

Kosutic, D., & Pigni, F. (2022). Cybersecurity: investing for competitive outcomes. *Journal of Business Strategy, 43*(1), 28-36.

Lu, Y., & Da Xu, L. (2018). Internet of Things (IoT) cybersecurity research: A review of current research topics*. IEEE Internet of Things Journal, 6(2)*, 2103-2115.

Makridis, C. A. (2021). Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018. *Journal of Cybersecurity, 7*(1), tyab021.

Michael, K., Kobran, S., Abbas, R., & Hamdoun, S. (2019, November). Privacy, data rights and cybersecurity: Technology for good in the achievement of sustainable development goals. In *2019 IEEE International Symposium on Technology and Society (ISTAS)* (pp. 1-13). IEEE.

Paananen, H., Lapke, M., & Siponen, M. (2020). *State of the art in information security policy development. Computers & Security, 88*, 101608

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & security, 31*(4), 597-611.

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: tensions in privacy and data. *Journal of the Academy of Marketing Science, 50(6)*, 1299-1323.

Richards, N., & Hartzog, W. (2020). A Relational Turn for Data Protection?. *Eur. Data Prot. L. Rev., 4*, 492.

Shackelford, S. J. (2019). Should Cybersecurity be a human right: Exploring the shared responsibility of cyber peace. *Stan. J. Int'l L., 55*, 155.

Tashtoush, Y. M., Darweesh, D. A., Husari, G., Darwish, O. A., Darwish, Y., Issa, L. B., & Ashqar, H. I. (2021). Agile approaches for cybersecurity systems, IoT and intelligent transportation. *IEEE Access, 10*, 1360-1375.

Wong, L. W., Lee, V. H., Tan, G. W. H., Ooi, K. B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities*. International Journal of Information Management, 66*, 102520.