Protecting the Edge:

Unveiling the Crucial Role of Cybersecurity

Lead Author: Ashleigh Stampp, Research Assistant

Co-authors: Devante Hines, Helpdesk Assistant

Christina Williams, Legal Intern

Shaheem Deans, Undergrad Research Intern

Abstract

As online technologies continue to advance, it becomes increasingly important to develop policies that ensure robust levels of cybersecurity. This essay explores the evolving capabilities and opportunities of online technologies and how policies can be developed to maintain security in this dynamic environment. It examines the challenges presented by edge devices and the Internet of Things (IoT) and explores the concept of "security by design." Additionally, it discusses the agility of policy development and its ability to prevent the misuse of data flowing across networks. By addressing these topics, we can better understand the complexities of cybersecurity on the edge and identify strategies to mitigate risks effectively. In consideration of the complexities presented by edge devices and the IoT; this essay will explore the development of policies that are necessary to safeguard cybersecurity on the edge.

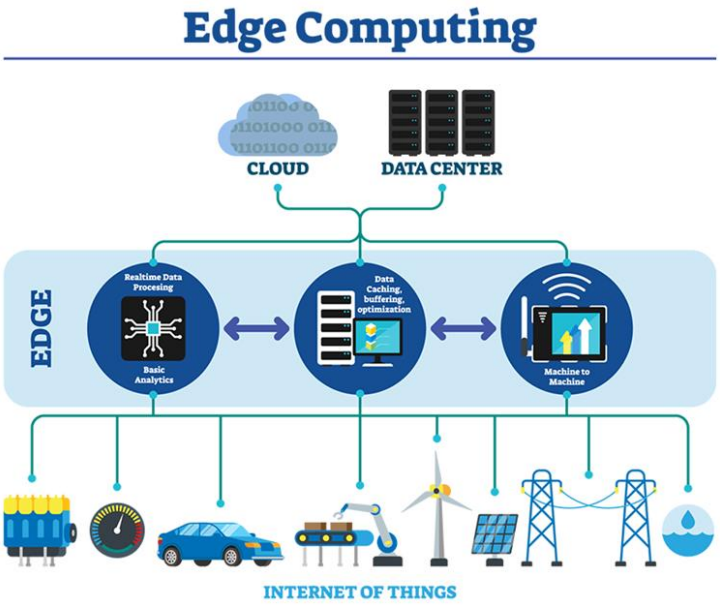
The Growing Significance of Cybersecurity

Cybersecurity encompasses the safeguarding of networks, devices, and data against unauthorized access or illicit activities. It involves employing the principles of *confidentiality*, *integrity*, and *availability* to ensure the protection of information. Cybersecurity has increasingly become important as emerging technologies such as artificial intelligence, the internet of things (IoT), virtual reality, and augmented reality proliferate, new risks and vulnerabilities have also emerged which need to be addressed and monitored. Moreover, as human beings interact with electronic devices or cyberspace, it leaves a digital footprint for each individual. Therefore, policy development plays a crucial role in managing these interactions as it ensures that robust levels of security are maintained, protecting individuals, organizations, and critical infrastructure from cyber threats.

What is Edge Computing?

Edge computing is an emerging computing paradigm which refers to a range of networks and devices at or near the user. While there isn't a specific date for its emergence, it gained attention and recognition as a viable computing paradigm. According to Shalom (n.d.), edge computing is a concept that can be traced back to the 1990's when Content Delivery Network (CDN) was launched by Akami. Edge Computing entails processing data closer to where it is being generated, enabling processing at greater speeds and volumes, leading to greater action-led results in real time (Accenture, n.d.). The growth of Internet of Things (IoT) devices and the need for real-time data processing at the edge of the network contributed to the rise of edge computing. Since then, it has continued to evolve and gain prominence in various industries and applications. See Figure 1, a diagram illustrating real-life edge computing use cases as provided below (Innovation at Work, n.d.).

Figure 1: Diagram Showing The Process of Edge Computing



Source: (Innovation at Work, n.d.)

Edge Computing Benefits & Limitations

Edge computing has many benefits, including lower latency, higher security, and improved efficiency. However, there are inherent risks of security and privacy issues in edge computing networks that place the end user's personal data at risk. For example, edge nodes exist nearer to users which results in reception of large amounts of sensitive data. If any of this data is stolen, it may result in instances of identity theft and more so very severe reputational damage for businesses.

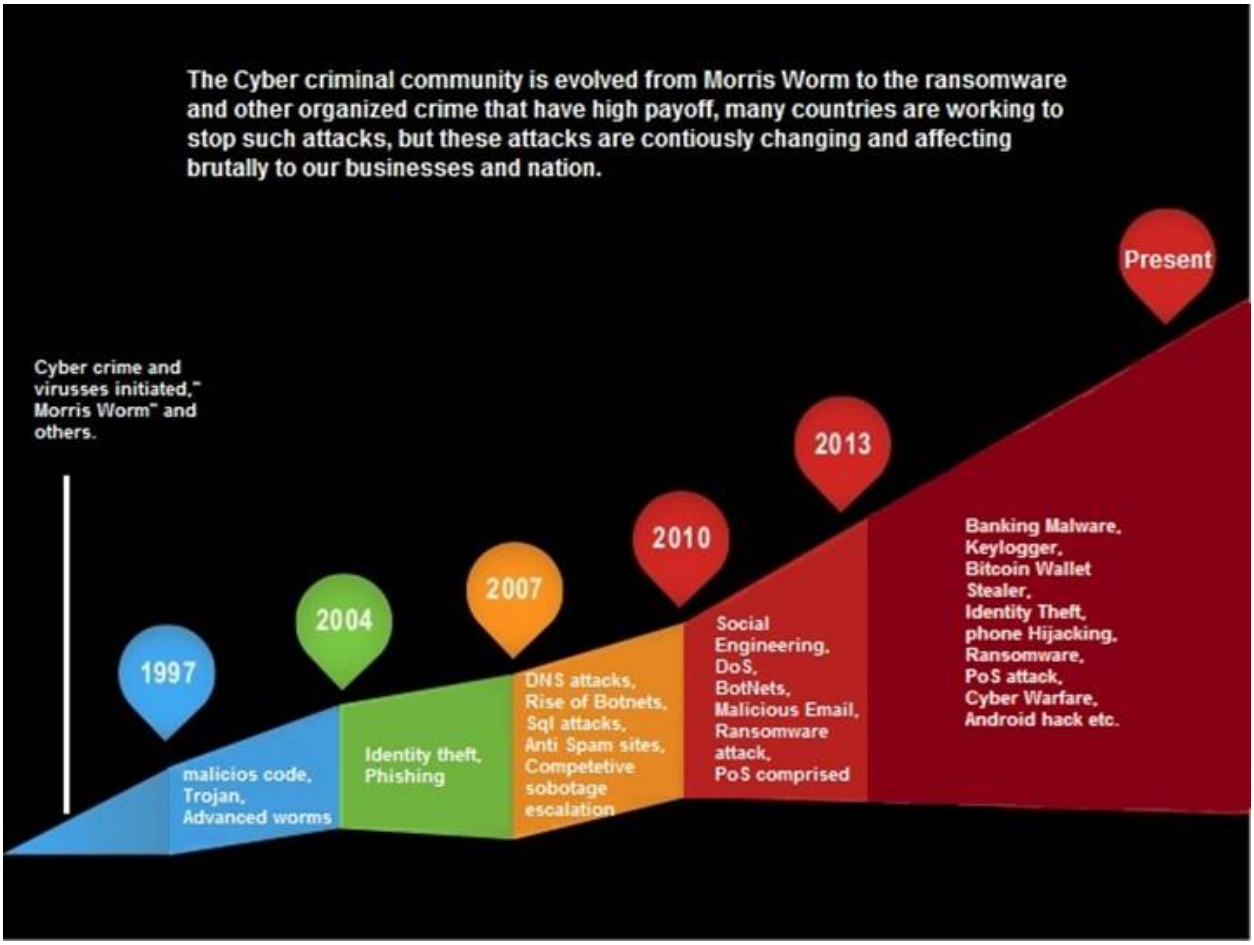
Edge computing network consists of a dynamic environment which is constantly changing. As a result of this, attackers can easily become part of the group. Moreover, it is very difficult to create

security rules for dynamic networks. Security rules are difficult to implement within a dynamic network due to the complexities, unpredictability, and rapid change of these systems. Privacy issues within this topology are fragile security techniques and algorithms, unsafe communication sessions between devices, difficulty in recovering data when there is a loss of power, lack of proper network visibility and lack of user's selective data collection. According to Alwakeel (2021), edge computing presents various security and privacy concerns. Few examples of attacks on the network of edge computing include Eavesdropping; Distributed Denial of Service Attack; Data Tampering Attack, False Data Injection and more. Furthermore, similar to cloud computing, edge computing also possesses limited network resources which do not support complex encryption algorithms.

The Evolution of Cyber Criminal Activity

Criminal activity often emerges in areas where valuable information can be obtained for financial or personal gain. With the rise of the digital economy, cybercriminals have found an ideal environment for their illicit activities. They exploit the internet and the abundance of information available online to carry out identity theft and engage in social engineering tactics. These tactics allow them to deceive individuals and manipulate them into providing sensitive information or engaging in actions that can lead to financial harm or data breaches. Therefore, to respond to this risk, cybersecurity has emerged to combat the issues faced as a result of cyber-criminal activities.

Figure 2: Diagram Showing the Evolution of Cyber Criminal Activity



Source: (Infosec Institute. (n.d.).)

The evolution of cyber-criminal activity has witnessed a significant transformation, progressing from early instances like the Morris worm to the sophisticated ransomware and other cyber-attacks prevalent today. In 1988, the Morris worm became one of the first notable instances of a widespread cyber-attack. It infected thousands of computers, causing system disruptions and highlighting the vulnerabilities of interconnected networks (Okta, n.d.). As technology progressed, cybercriminals started utilizing increasingly complex methods, taking advantage of the expanding accessibility and interconnectedness of the internet.

In today's world, ransomware attacks have emerged as a dominating and increasingly profitable form of cybercrime. In these attacks, nefarious individuals encrypt the data of victims and request a ransom in exchange for its decryption and release. They have wreaked havoc on industries ranging from healthcare to finance, leading to financial losses and compromised data security. Furthermore, cyber criminals have broadened their tactics to include phishing attacks, social engineering, and other forms of cyber-attacks, leveraging human vulnerabilities and sophisticated hacking tools and techniques to breach networks, steal sensitive information, and conduct large-scale cyber espionage operations.

To address the escalating risks posed by cybercriminal activities, the field of cybersecurity has emerged as a critical defense mechanism. Cybersecurity specialists constantly adapt and develop creative techniques to identify, prevent, and mitigate cyber threats in response to the evolving tactics used by cybercriminals. To enhance network defenses and secure sensitive data, they use modern technology such as intrusion detection systems, firewalls, and encryption algorithms. Furthermore, cybersecurity professionals put in place strong authentication systems, safe coding practices, and staff awareness programs to address human vulnerabilities and reduce the chance of successful social engineering and phishing attacks.

Policy Approaches

The proliferation of digital platforms, cloud computing, and the Internet of Things (IoT) has transformed various sectors, including healthcare, manufacturing, transportation, and communication. These capabilities and opportunities provided by these online technologies have expanded exponentially over the years but while these advancements have improved efficiency,

connectivity, and accessibility, they have also opened new avenues for cyber threats and attacks. Therefore, as online technologies evolve, policymakers must adapt their strategies to address emerging challenges and protect the integrity and security of digital systems. This raises the question of which approach would best combat the risk associated with the use of these technologies.

Security by Design

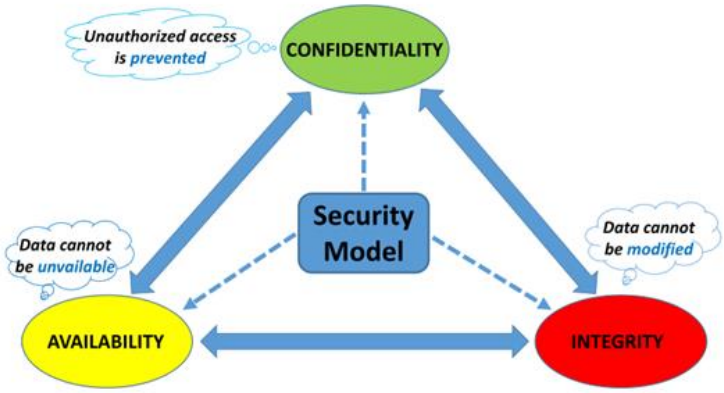
Security by design is an approach to developing and designing systems, products, and applications with security as a fundamental aspect from the initial stage of the development process. It involves integrating security considerations and measures into every stage of the design, development, and implementation of a system or product. By incorporating security into the design phase, security by design promotes a proactive rather than reactive approach to cybersecurity. Examples of the application of security by design principles may be incorporated into the Internet of Things (IoT) devices, autonomous vehicles, blockchain technology, cloud computing, and mobile applications as these become more prevalent in homes and businesses. Embracing security by design principles from the initial stage ensures that security is not an afterthought but an integral part of the entire development lifecycle.

Confidentiality, Integrity, Availability (CIA) Triad

The Confidentiality, Integrity, Availability (CIA) Triad is a model which is widely used and accepted as a fundamental concept in the development of information security. It may be used for

identifying vulnerabilities and opportunities for formulating solutions to cybersecurity problems (Fortinet. (n.d.).).

Figure 3: Diagram Showing CIA Triad



Source: CryptIoT. (n.d.).

In a scenario where the available data is compromised, there may be systems in place that can be used to withstand or maintain the confidentiality aspect of the model. The information gathered can be leveraged to identify and rectify vulnerabilities and to adopt effective strategies and practices that have yielded positive outcomes in other instances. This approach may be used within the context of online banking systems as they must prioritize confidentiality in order to ensure that customer information such as account numbers, passwords, and personal details remain protected and accessible only to authorized individuals. Integrity is also important in online banking as it ensures that customer data and transactions remain accurate, reliable and unchanged. Similarly, availability is crucial in ensuring that customers may access and use online banking services as needed. This comprehensive approach helps build trust, safeguards against unauthorized access or

modifications, and provides a secure and reliable online banking experience for customers. It is imperative therefore for governments to align their policies with the principles of the CIA triad.

Omni-stakeholder Approach to Policy Development

Effective cybersecurity policies ought to be a shared responsibility that requires collaboration among stakeholders, including government agencies, industry experts, and the academic community. This approach must promote collaboration, inclusivity, and information sharing to improve threat intelligence, develop best practices, and enhance incident response capabilities. While policies themselves may not provide solutions to problems; and may even cause challenges if not well-defined and followed, policies do specify the intended goal that all organizational initiatives should strive for. According to the National Center for Education Statistics (n.d.), security policy by definition refers to clear, comprehensive, and well-defined plans, rules, and practices that regulate access to an organization's system and the information included in it.

A good example of an omni-stakeholder approach to policy development is Public-private partnerships. These collaborations can play a crucial role in creating a unified approach to cybersecurity as it leverages the expertise and resources of multiple entities. Vendor partnerships is another effective way to develop policy as partnerships between vendors and suppliers ensure that security is embedded in the design and manufacturing processes of edge devices and the IoT components as it involves establishing security requirements, conducting security audits, and regular updates and patches.

Furthermore, policymakers should actively engage in international discussions and efforts to establish cyber norms and rules of behavior. This includes participating in international forums, such as the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications, to promote responsible state behavior and deter cyber-attacks.

In summary, encouraging collaboration and information sharing among government agencies, private sector entities, and international partners is essential for staying ahead of evolving threats. Policymakers should therefore promote public-private partnerships, industry collaboration, and international cooperation to exchange threat intelligence, share best practices, and coordinate responses to cyber incidents.

Regulatory Frameworks

Regulatory frameworks are essential for establishing minimum security requirements and standards across industries. They should incentivize organizations to adopt best security practices by incorporating security into the design, development, and implementation of technologies and focus on scalable security solutions that can be easily deployed and managed across numerous devices. Some of these minimum standards should include the following:

1. Threat modeling which facilitates the identification of potential threats and risks specific to the system and its components. It should consider possible attack vectors, vulnerabilities, and potential impacts on interconnected systems.

2. Secure, resilient architecture that incorporates appropriate security controls. This includes secure communication protocols, access controls, encryption, authentication mechanisms, and secure storage and processing of sensitive data.
3. Interoperability within complex networks with various interconnected devices and systems. Since achieving interoperability while maintaining security can be challenging, standards and protocols must be implemented consistently and securely across different devices and platforms.
4. Mechanisms that continuously monitor and update on devices and networks, including intrusion detection systems, security event logging, and anomaly detection. Additionally, regular updates and patches must be applied promptly to address vulnerabilities and protect against emerging threats. For example, in Jamaica, the Data Protection Act mandates that incidents must be reported within 72 hours, such mechanisms may facilitate this timely report and intervention.

Therefore, by setting regulatory standards, policymakers can encourage security by design and mitigate the risks associated with emerging technologies.

Cybersecurity Education and Awareness Programs

Additionally, policy development should prioritize cybersecurity education and awareness programs. By fostering a culture of cybersecurity fundamentals, individuals and organizations can better understand the risks they face and take proactive measures to protect themselves. Users should understand the risks associated with the IoT devices, such as weak passwords, default settings, and potential privacy concerns. Therefore, to fully adapt and thrive in the ever-evolving

landscape of the fourth industrial revolution, it is crucial to prioritize and significantly enhance Digital Media and Information Literacy (DMIL) skills.

Policy Approach to Preventing Misuse

The ability of policy to develop quickly enough to prevent misuse of data flowing across networks depends on various factors, including the specific context, the nature of the data, and the agility of policy-making processes. The following are other limitations:

Technological advancements: The rapid pace of technological advancements makes it challenging for policy to keep up with the evolving landscape. New technologies, such as artificial intelligence and blockchain, introduce novel ways of processing and sharing data, requiring policy frameworks to adapt quickly.

Regulatory frameworks: Governments and regulatory bodies play a crucial role in establishing policies and regulations to govern data usage. However, the process of formulating and implementing new policies can be time-consuming and complex, often involving multiple stakeholders and public consultations. As a result, policymaking may lag behind technological developments.

International coordination: Data flows transcend national boundaries, necessitating international coordination and cooperation to effectively regulate data misuse. Harmonizing policies across different jurisdictions can be challenging due to varying legal systems, cultural differences, and

conflicting interests. As well as achieving consensus on global data governance frameworks can be a lengthy process.

However, taking into account the following considerations could increase the responsiveness of policy to the misuse of data:

Proactive approaches: Policymakers can adopt proactive approaches to address the challenge of data misuse. This includes anticipatory policymaking that takes into account emerging technologies and potential risks. Proactive policies may involve creating flexible frameworks that can be adapted to new developments and collaborating with industry experts to stay informed about technological advancements.

IT Governance and Security Governance: Incorporating robust IT Governance and Security Governance practices can significantly enhance the effectiveness and responsiveness of policy in addressing data misuse. IT Governance ensures that the organization's IT systems and processes align with its overall objectives and strategies. Similarly, Security Governance focuses specifically on managing and protecting information assets. By incorporating IT Governance and Security Governance practices into the policy-making process, organizations can enhance their ability to prevent data misuse. Policy regulations should govern the collection, storage, processing, and sharing of data, ensuring transparency, consent, and accountability. By providing individuals with control over their data and imposing penalties for non-compliance, policies can deter unauthorized data access and misuse. These practices provide a structured approach to aligning IT systems, managing risks, implementing security controls, and maintaining the agility necessary to respond effectively to the ever-changing landscape of data flow across networks.

Conclusion

Cybersecurity on the edge is a complex and evolving domain. While the interconnectivity offered by edge devices and the IoT presents significant challenges, effective policy development is critical to strike a balance between innovation and security especially in a small island developing state where there needs to be the consideration of interdependencies within networks. Policies should therefore encompass robust data privacy and protection regulations that foster collaboration, promotes education, implements regulatory frameworks, encourages international cooperation and maintains agility. Therefore, through this comprehensive approach, policymakers can enhance the security of networks and prevent the misuse of data which allows consumers to navigate the evolving cyber landscape with confidence as countries reap the benefits of technology while safeguarding digital ecosystems.

References

Alwakeel, A. M. (2021). An Overview of Fog Computing and Edge Computing Security and Privacy Issues. Sensors, 21(24), 8226. https://doi.org/10.3390/s21248226

Accenture. (n.d.). What is Edge Computing & Why is it important? Retrieved from https://www.accenture.com/us-en/insights/cloud/edge-computing-index#:~:text=Putting%20compute%20at%20the%20edge,equipment%20data%20and%20automated%20retail

CryptIoT. (n.d.). Security Solution for IoT Communication Protocol. Retrieved from https://cryptiot.de/iot/security/security-solution-iot-com-protocol/

Fortinet. (n.d.). CIA Triad. Retrieved from https://www.fortinet.com/resources/cyberglossary/cia-triad#:~:text=The%20three%20letters%20in%20%22CIA,and%20methods%20for%20creating%20solutions

Infosec Institute. (n.d.). Evolution in the World of Cyber Crime. Retrieved from https://resources.infosecinstitute.com/topic/evolution-in-the-world-of-cyber-crime/

Innovation at Work. (n.d.). Real-Life Edge Computing Use Cases. Retrieved from https://innovationatwork.ieee.org/real-life-edge-computing-use-cases/

National Center for Education Statistics. (n.d.). Chapter 3: Security in Networked Computing Environments. Retrieved from https://nces.ed.gov/pubs98/safetech/chapter3.asp

Okta. (n.d.). Morris Worm. Identity 101. Retrieved from https://www.okta.com/identity-101/morris-worm/

Shalom, N. (n.d.). What is edge computing? Opensource.com. Retrieved from https://opensource.com/article/17/9/what-edge-computing#:~:text=Edge%20computing%20can%20be%20traced,such%20as%20images%20and%20videos