Economics of Cybersecurity II: Stakeholders

By: Natalia Khaniejo
Edited: Amber Sinha

Introduction

The cybersecurity ecosystem has several stakeholders involved such as the companies from various sectors of the economy, the ISPs, the software vendors, users and the government. Therefore, there are varying levels at which Cybersecurity needs to be addressed. Determining the levels of investment required for each of these stakeholders has proved complex and challenging as the incentives driving investment at each stakeholder level vary. Furthermore, the problem that stakeholder separation creates is that infrastructures and networks are no longer silos that can exist independent of each other. The risk associated with each level of Cybercrime – individual, organizational, sectoral and national – can no longer be segregated into neat silos.

While each layer of the infrastructure may require a different form of securitization, the consequences of data and financial breaches are no longer limited to the targeted victims. Furthermore, given the increased emergence of smart devices and their amalgamation with the network, isolated security measures and blind investments are often insufficient as there may be multiple points of attack within the network that might not require access to an endpoint device at all. Wannacry and Petya are two small examples of the extent to which cyber-frameworks are interconnected and interdependent. Another example of this interconnected infrastructure can be seen in the fact that entire healthcare systems, social welfare systems, critical infrastructures, etc. are all vulnerable in the case of a cyberattack.

Nonetheless despite these interconnections, determining collaborative methods of cybersecurity investment has proved to be a key challenge. There has been a rise in Public-Private partnerships but given that the minimum cost of 'required'

investment for expected reward[1] would be lesser for organizations securing their endpoint nodes and higher for governments breach proofing their critical infrastructure finding common ground towards security investment between the two becomes difficult. Furthermore, the types of attacks committed against each sector vary greatly and therefore the role to be played by each stakeholder in contributing towards a secure cyber architecture – from governments and private corporations to ISPs and software vendors – needs to be reassessed as well. The biggest concern in blanket security strategies and investments is that, while all of these varying stakeholders partake of and participate within the same network – not including individual variations of cordoned off network infrastructures – the risk calculus and cost of breach would vary significantly across stakeholders. "the types of information security desired by the government may be different from those that individual firms might consider. It is reasonable to assume that information security solutions needed for the public welfare are different (and possibly more stringent) than those required by firms."[2] This section will attempt to examine the varying cybersecurity challenges at the government and private sector level.

Cybersecurity from a government perspective

The emergence of Critical Information Infrastructures and their increasing coalescence with ICTs has necessitated government investment in Cybersecurity. Most countries have responded by developing not just a National Security Strategy, but also a Cybersecurity strategy. Furthermore, countries across the world are increasingly realizing the need for investing in cybersecurity with bodies like the ITU and the world economic forum both making security a key concern. According to the 2017 Global Cybersecurity Index, several countries have established CERTs – national as well as sectoral – and begun instituting legislation around data breaches and cybercrimes.[3] However, aside from securing broad cyberspace boundaries, governments don't seem to be doing as much as they need to, towards building better policies and encouraging healthier cyber ecosystems. In the paper *The Economics of Cybersecurity*, Alderson and Soo Hoo point to the more non implementable standards measures being recommended by governments. They state that "Government policy makers continue to shy away from traditional regulation as a solution, preferring instead to rely on non-coercive measures to encourage and entice stakeholders into securing the infrastructure."[4] They refer to practices such as i) Leading by example, ii) Funding

[1] In this case maximum possible security at minimum possible cost.
[2] Dynes, S., Goetz, E., & Freeman, M. (2007). Cyber Security: Are economic incentives adequate? International Conference on Critical Infrastructure Protection. Springer.
[3] ITU. (2017). Global Cybersecurity Index. ITU.
[4] Alderson, D., & Soo Hoo, K. (2004). The Role of Economic Incentives in Securing Cyberspace. Center for International Security and Cooperation.

Research iii) Establishing Standards iv) Encouraging Information Sharing v) Evangelizing[5] and state that while such measures may have been helpful to small extents, they have largely been ineffective in providing systematic direction towards the adoption of policy best practices. Public-Private partnerships have been fraught to say the least, primarily due to the differing incentives motivating the two sectors. Given that most Cyberinfrastructure – and innovation in the realm – is being funded by Private stakeholders, Governmental regulations have been advisory at best, aside from a base level of compliance measures which tend to become outdated sometimes even before they are enforced.

Furthermore, sometimes governments tend to err on the side of caution and create regulatory mechanisms that are unable to stand the increasingly nuanced attack spectrum that is emerging in the current day and age. Data localization demands, and other such attempts at keeping information secure would demand an equal investment in developing efficient infrastructural capabilities. Furthermore, bureaucratic processes would also need to be updated to stay abreast of the changes taking place in the regulatory landscape in order to ensure that companies and users don't get caught in procedural quagmires. For example, within the FinTech landscape itself, if regulatory policies are to be established, there would need to be a graded system regarding the applicability of standards to companies. If regulations are overwhelming, they could serve as deterrents and end up stopping innovation altogether, but if they are undefined and amorphous, companies might not comply with recommended standards at all thereby creating multiple vulnerabilities and loopholes. While governments are increasingly depending on private companies for infrastructural and industrial investment, what needs to be remembered is that at the end of the day, private stakeholders will primarily be driven by profit motivations instead of altruistic social necessities. "Government, as the defender of the public interest, is accorded both the responsibility and the power to reshape the market to foster a more secure infrastructure."[6]

Private Stakeholders

By concentrating primarily on regulatory and advisory roles, most governments have adopted a collaborative approach to the task of cybersecurity, choosing to concentrate on building public-private partnerships in order to mitigate threats. As Alderson points out, the idea behind such an approach is "that the mutual need for a robust cyber infrastructure with appropriate government oversight will naturally foster cooperation among key players."[7] The key difference that emerges

[5] *Ibid*.
[6] Alderson, D., & Soo Hoo, K. (2004). The Role of Economic Incentives in Securing Cyberspace. Center for International Security and Cooperation.
[7] *Ibid*.

however, is that while private companies and stakeholders are equally invested in developing secure infrastructures, they tend to privilege shareholder and consumer motivations, engaging in as much research/investment as will tide over their needs. Social losses then take a backseat in an analysis regarding what security is to be privileged for the firm itself. Furthermore, while private stakeholders may be more focused on financial security, they may be less stringent with data security leaving the network vulnerable. Software companies also choose a roll out now, patch later method while dealing bugs in the system without taking into consideration the larger damage such actions could cause.

Given the expensive nature of cybersecurity today, most companies would attempt to gain maximum possible benefit with minimum possible expenditure. Using the prisoner's dilemma to describe this phenomenon, Douglas Kelly takes the example of two companies, A & B and explains how, if A were to invest heavily in cybersecurity, B would be able to freeload on the reputational costs, thereby receiving maximum security for minimal investment. The reverse stands to reason if the roles are switched as well. However, the issue arises when both decide to freeload instead of investing in cybersecurity thereby causing a dangerous vulnerability. Furthermore, Kelly states, "With two companies, an efficient outcome could result if transaction costs are low; however, a multitude of companies would encounter these same incentives and transaction costs would likely be high"[8] which becomes a further disincentive for companies to invest in cybersecurity beyond minimal levels. Another economic model that is often used to determine the amount of recommended investment is determined according to the proportion of low threats, and sophisticated threats. Gilligan recommends implementing comprehensive baseline security to tackle the former and aspiring towards security investments that move beyond these baseline controls in order to tackle sophisticated threats.[9]

The cost of Cybercrime report states that there are three key sectors of investment that companies should focus on in order to secure themselves from potential threats. These are:

1) Investing in "brilliant basics" namely 'security intelligence and advanced access management' while keeping these processes open to innovation and experimentation in order to ensure protection against evolving threats

2) Reduced reliance on minimum compliance levels and increased pressure testing towards vulnerability identification

[8] Kelly, D. (2017). The Economics of Cybersecurity. 12th International Conference on Cyber Warfare and Security 2017 Proceedings. Ohio: Academic Conferences and Publishing Limited.
[9] Gilligan, M. J. (2013). The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment. Retrieved from AFCEA Cyber Committee: http://www.afcea.org/mission/intel/documents/EconomicsofCybersecurityFinal10-24-13.pdf.

3) Balanced spending on new technologies such as analytics and artificial intelligence towards enhanced scale value.[10]

While such measures would work towards the protection of the industrial value chain, it would also be helpful for companies to consider the benefits of investing in social externalities as well. Bruce Kobayashi states that "private and social incentives to provide investments in security diverge due to an inability to internalize positive and negative externalities generated by private security investments."[11] Furthermore, the lack of any onus or responsibility on the company in the case of a data breach, makes them less willing to consider expanding their cybersecurity investments beyond minimal infrastructural and compliance requirements. This is where Government subsidies, land allocations, tax benefits, and other such incentives would encourage companies to consider expanding their security repertoire and invest in cybersecurity as a public good.

[10] Ponemon Institute, A. (2017). Cost of Cybercrime. Ponemon Institute.
[11] Kobayashi, B. H. (2005). Private versus Social Incentives in Cybersecurity, Law and Economics. In M. Grady, & F. Parisi, The Law and Economics of Cybersecurity. New York: Cambridge University Press.