Economics of Cybersecurity IV: Regulatory Mechanisms

By: *Natalia Khaniejo*
Edited by: Amber SInha

Introduction

While securing cyberspace there is a need to examine whether the measures being taken are preventive or responsive - do they stop attacks or deter attackers - as well as whether they are proactive or reactive - do they occur in reaction to an event or actively seek out and prevent potential future events. There needs to be a holistic balance to any security strategy being constructed that includes most if not all these aspects. Another key consideration that needs to be factored while determining the efficacy of proactive/preventive cybersecurity measures and reactive cybersecurity strategies, is cost efficacy. The book *Cyber Security: Economic Strategies and Public Policy Alternatives*[1] looks at these measures at length. While analyzing the benefits and costs of each approach, Gallagher, Link and Rowe find that while "a proactive strategy, in general, leads to fewer cyber security breaches, in some instances a reactive strategy may be more cost-effective." Another axis along which proactive and reactive strategies are measured is in the case of dealing with human factors as well as technical factors. While some proactive measures – such as staff training, education, reskilling – may prove helpful in deterring attackers as well as sussing out threats at a preventive level, creating blockades against every single virus, bot, worm, etc. might become expensive and unsustainable. From a technical perspective, it is also difficult to create a total blockade against such threats as the nature of the threat is constantly evolving. In such cases limiting the damage caused by the attack tool and developing segregation strategies to prevent it from infecting other sectors/networks would wield better results in the long run. Aside from individual and organizational investment there are also certain regulatory

[1] Rowe, B., Link, A. N., & Gallaher, M. P. (2006). Cyber Security: Economic Strategies and Public Policy Alternatives. Cheltenham: Edward Elgar Publishing Ltd.

mechanisms that exist towards safeguarding systems and reducing cyberthreats. Some of these regulations are examined below.

Ex Ante Safety Regulation vs. Ex Post Liability measures

Regulation within the realm of cybersecurity is limited to say the least. Nonetheless, currently there are two primary approaches that are used while dealing with Cybersecurity and Cybercrime. One is the Ex Ante safety approach and the other is the Ex Post Liability model of regulation. Ex Ante is designed to prevent accidents by prescribing safeguards before accidents occur. They serve as proactive and preventive measures that would attempt to deter attackers from attempting the crime in the first place. Currently, majority of the information and internet security practices that exist are compliance-driven and therefore Ex-Ante in nature. Within this umbrella, firms adopt systematically recommended 'best practices' in order to test their own compliance. Therefore, data security provisions under the Section 43A Rules in the Information Technology Act,[2] or those contemplated in the Sri Krishna Committee White Paper[3] are essentially in the nature of ex ante regulations which would oblige data controllers to "protect the security and confidentiality" of customer information by putting into place adequate security safeguards.

These safeguards primarily rely on due process and compliance standards that would encourage companies to incorporate a fixed system of requirements into their security policy and implement procedural mechanisms for reporting incidents. These measures tend to be less dependent on constantly changing technologies as they form minimum standards and regulations that can be adopted in rapidly changing technological environments as well. Furthermore, it is usually argued that such processes would also be easier to regulate as compliance verification would not require technical complexity and verifying whether or not standards are being applied would become easier for regulators. However, this very ease of supervision is what has made security researchers question the efficacy of such policies.

The alternative to these measures is to assign ex post liability mechanisms. These are based on attributing responsibility and defining clear culpability in the case of a breach or attack. It is hoped that a clear chain of responsibility and liability will encourage actors within the network to be more careful and maximise security protocol. Ex post liability regulation aims to increase responsibility by using successful attribution tactics and broadly reducing "(a) the likelihood of such

---

[2] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. https://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf.

[3] http://meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited.

attempts, (b) the likelihood that such attempts will succeed should they take place, and (c) the expected consequences of such activities."[4] These measures would be particularly useful in the case of software companies and ISPs. Software companies in particular are rarely held responsible for security vulnerabilities. The recent Microsoft attack is an example of the ways in which these vulnerabilities are capitalized on in the absence of liability. Several scholars have argued for making software companies responsible for damages that occur through vulnerabilities in their software, however, if this is blatantly imposed onto the proprietary good, it could cause two key issues. Companies might reduce innovation in order to avoid running into legal hassles – concomitantly developers would also be less invested in innovating features as it might lead to critical vulnerabilities and the person responsible for the code might become the sacrificial pawn for the company to save face. Conversely, companies might also increase the price of licensed software thereby creating an unequal and dangerous swing in the cost of security. While licensed softwares are currently rolled out in various versions with the price dependent on access to updates, this might get worse if the companies are to be held liable as they might cushion their profit margins by charging their consumers exorbitant prices as collateral damage. Legal scholars have studied these mechanisms in great detail and found that the most efficient model involves a delicate balance between the two.

The key issue between establishing such mechanisms successfully at the moment is that there is a distinction between the policy framer and the policy user. As Alderson and Soo Hoo state "the fundamental problem behind the current infrastructure vulnerability is that the economic incentives for both makers and users of Internet technology are not aligned to compel the vigilant development, deployment, and application of secure technology."[5] These policies are usually made and supervised by people with little to no technical proficiency and therefore these measures suffer from under or over-security. Given the lack of information and disclosure regarding data breaches, it is also difficult for policy makers to keep track of the most up to date vulnerabilities around which regulation needs to be shaped. All these reasons, collaboratively lead to either an oversecuritized environment that stops and throttles innovation or an undersecured realm with vague supervisory recommendations and the lack of a liability chain.

[4] Cordes, J. J. (2011). An Overview of the Economics of Cybersecurity and Cybersecurity Policy. CSPRI.

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

Cyber-insurance

Research around cyber-insurance is primarily predicated around examining the ways in which Cybercrime and concomitantly cybersecurity manifest. Researchers such as Rainer Bohme, Gaurav Kataria,[6] Galina Schwartz,[7] Jean Bolot, Mark Lelage,[8] etc. have all examined the possibilities of incentivizing cybersecurity through an insurance model. Given the rapidly evolving technological landscape and the more or less equal availability of infrastructure for malicious attackers as well as defenders, 'absolute security' is impossible. A key example of the insurance model is the Obama Administration's attempt at developing and curating incentives for cybersecurity insurance in 2014. The intent underlying the development of a cyber-insurance market was that it would reduce cyber risk, by decreasing the reward to be gained at the end of a completed attack. Furthermore, the transfer of financial risk to third parties has been a point of particular interest since the Y2K scare.

In the paper *Modelling Cyber-Insurance: Towards a Unifying Framework,* Bohme and Schwartz trace the shift in the theorization of a potential insurance market that has occurred. They state that early works in the 1990s focused on the "general merits of cyber-insurance or protocols borrowed from digital cash to enable risk re-allocation in distributed systems... ...In the late 1990s, when the business perspective of information security became more prominent, visions of cyber-insurance as risk management tools were formulated."[9] However, in terms of practice, the lack of synthesis in the realm has caused a stagnation of most policy incentives and thereby thwarted the development of a feasible insurance strategy. The authors present instead a unifying framework that attempts re-envision cyber-insurance by breaking "the modeling decisions down to five key components: (1) network environment, (2) demand side, (3) supply side, (4) information structure, and (5) organizational environment."[10] They argue that a robust cyber-insurance market would be tremendously beneficial to society and mitigate a significant amount of the losses incurred in cyberattacks on a fairly regular basis. Furthermore, it is also believed that a healthy insurance market would create a sense of responsibility in individuals as well as organizations and encourage them towards investing in necessary security measures. If enough insurance companies emerge in the market, security premiums would gradually

[6] Bohme, R., & Kataria, G. (2006). Models and Measures for Correlation in Cyber-Insurance. Workshop on the Economics of Information Security (WEIS) University of Cambridge, UK.
[7] Bohme, R., & Schwartz, G. (2010). Modeling Cyber-Insurance: Towards A Unifying Framework. Workshop on the Economics of Information Security (WEIS). Harvard.
[8] Bolot, J., & Lelarge, L. (2008). Cyber Insurance as an Incentive for Internet Security. WEIS 2008, Seventh Workshop on the Economics of Information Security, Hanover NH (USA).
[9] Bohme, R., & Schwartz, G. (2010). Modeling Cyber-Insurance: Towards A Unifying Framework. Workshop on the Economics of Information Security (WEIS). Harvard.
[10] *Ibid*.

decrease thereby further encouraging cybersecurity investment. Furthermore, in order to ensure that claimants and incidents are genuine - and given the fact that the competitive advantage for insurance companies is based on a risk-adjusted premium differentiated model – security companies would also be invested in gathering data on the incidents and thereby reducing the information asymmetry currently prevalent in the market.

There are several reasons why the cyber-insurance market hasn't picked up on the whole, despite these benefits.[11] Information asymmetry continues to be a key barrier with insurers claiming that the absence of breach disclosure makes it impossible to provide realistic insurance estimates.[12] Information regarding security measures being adopted by companies, the true estimate of damages caused in the case of a cyberattack, and the clear demarcation of responses taken in the aftermath of the cyberattack are all extremely essential nodes in the development of risk/insurance strategies. Without this information, insurers would be unable to trace the contours of threats faced and the security investments required in response. Recommending legislation aimed at disclosing cyber-incidents would help create a cyber-risk map that would be extremely helpful in mitigating challenges in a holistic manner. A second key issue that emerges is the absence of a liability chain, and in the case of cyber incidents, who is to be blamed for what remains a key conundrum for most parties involved. Furthermore, in the absence of any firm legislature regarding these issues, providing insurance as well as securing assets from cyber attacks would be unrealistic and unsustainable to say the least.

Incentivizing cybersecurity

Incentivizing cybersecurity and the adoption of healthy cyber-hygiene would go a long way in developing a holistic network and security architecture. These measures towards better cybersecurity investment need to be undertaken by the public and private sector both. The private sector currently functions on the belief that the losses from cyber attacks do not equal the need for greater costs in cybersecurity. This fundamental misapprehension is responsible for lax security measures where companies, in the absence of liability mechanisms, choose to adopt convenient practices over necessary ones. Furthermore, in the cases where regulations are implemented, companies complain that they becomes so stringent that any form of growth or innovation gets fundamentally nipped in the bud. Unfortunately, market forces have failed to secure the sector by themselves and

[11] Woods, D., & Simpson, A. (2017) Policy measures and cyber insurance: a framework. Journal of Cyber Policy, 2:2, 209-226, DOI:10.1080/23738871.2017.1360927.
[12] Pal., R. (2012). Cyber-Insurance for Cyber-Security: A Solution to the Information Asymmetry Problem. SIAM Annual Meeting.

regulatory intervention is required in some measure to ensure that individuals are not left hanging in the cases of data and financial breaches. There are several ways in which this stasis can be countered.

1. Development of a more holistic regulatory framework that examines cybersecurity legislation from a balance between both - ex ante safety and ex post liability - perspectives.
2. Establishment of a liability framework that holds ISPs responsible for malware and breaches being proliferated on their domains.
3. Provision of incentives such as tax benefits, grants, land, etc. to encourage better cybersecurity practices and increase cybersecurity investments.
4. Making a certain minimal amount of information disclosure necessary to ensure that regulatory policies are being made keeping in mind evolving threats.
5. Establishing sectoral as well as national CERTs with clear directions regarding information sharing, as well as information disclosure.
6. Building better information sharing mechanisms and clear protocols in order to ensure that in the case of an attack companies know exactly whom to approach and for what purpose.

Such measures could improve cybersecurity hygiene and combat key barriers that prevent companies and individuals from taking responsibility for breaches caused by sheer callousness. These measures would require a certain amount of multi-stakeholder collaboration at the level of organisations as well as the government. However, these measures would certainly go a significant way towards protecting consumers and building better security frameworks.