Economics of Cybersecurity III: Barriers

Amber Sinha and Natalia Khaniejo

Interconnectedness of Network Infrastructure

Network infrastructure forms a major part of both Economic as well as technological analysis. It is the interdependent nature of network and communication infrastructures that jeopardizes as well as drives the cybersecurity environment today. In *The Economics of Cybersecurity: From the Public Good to the Revenge of the Industry*,[1] Danilo D'Elia states that the vulnerabilities identified today can be traced back to the fact that security was never an original concern for ICT developers. The inability to determine how these technologies would manifest and proliferate and the lack of securitization measures at the onset have led to a culture of callousness with individual as well as institutional data. The privileging of converged networks and interconnected infrastructure over rigorous testing and security practices leads to open vulnerabilities and unpatched servers. The last few years have witnessed a rise in the use of malware, ransomware, botnets that can paralyze systems and provide quick profits through the payment of cryptocurrency ransoms.

While cryptocurrencies are not pseudonymous, they provide a greater degree of anonymity than most digital financial trails do and determining and tracing these accounts would require more aggressive security maneuvers and investigations. This points to another key issue in which Cybersecurity differs from physical security - investigating cyber crimes might necessitate maneuvers that employ tools and processes used by the criminals themselves. The emergence of transnational economic and communication networks has led to a panicked reassessment of the need for security practices that don't transgress sovereign security standards and a safeguarding of financial and personal data. While explaining the twofold risk that has emerged by the lack of original security measures, D'Elia further states that "[d]ue to the interdependence of critical

[1] D'Elia, D. (2015). The Economics of Cybersecurity: From the Public Good to the Revenge of the Industry. Security of Industrial Control Systems and Cyber Physical Systems. Vienna: Springer.

infrastructures (CIs), the impact of an incident won't be limited to the original sector of activity nor to a nation."[2]

The interconnectedness is what drives the user numbers within the network up - for communication as well as commercial networks. A common theoretical tool used to analyze the functioning of networks – specifically telecommunication networks – is Metcalfe's Law. Named by the theorist George Gilder in 1993, the law states that "the effect of a telecommunications network is proportional to the square of the number of connected users of the system (n^2)." Theorists remain divided regarding the exact values of the function provided by Metcalfe in evaluating growth, and even question its validity in accurately defining growth parameters, however, it serves as an extremely useful tool through which to examine patterns of interconnectedness in the growth of information infrastructures. Theorists like Ross Anderson use this Law to talk about the burgeoning of telecommunication networks and devices and state that "while networks can grow very slowly at first… …once positive feedback gets established, they can grow very rapidly."[3] While citing the telephone, telegraph and the internet as examples Anderson further states that "the same principles apply to virtual networks, such as the community of users of a mass-market software architecture."[4]

However, conversely the growing interconnectedness and the values attributed to each new node in the network cannot be considered equal. The additional value attributed to the network with each new addition must be considered in terms of weighted averages. While refuting Metcalfe's law, Bob Briscoe, Andrew Odlyzko and Benjamin Tilly state that "only companies of roughly equal size are ever eager to interconnect. In most cases, the larger network believes it is helping the smaller one far more than it itself is being helped. Typically in such cases, the larger network demands some additional compensation before interconnecting."[5] This becomes a particularly interesting point while analysing how ISPs form connections. Smaller Service Providers in their keenness to connect with larger more expansive providers often don't demand that the former take responsibility for malicious zombie computers they might unknowingly and callously be supporting. Some surveys have found that "just 10 ISPs accounted for 30 percent of IP addresses sending out spam worldwide"[6] Reducing complete

---

[2] *Id*.
[3] Anderson, R. (2002). Why Information Security is Hard - An Economic Perspective. Computer Security Applications Conference. New Orleans: ASAC.
[4] *Ibid*.
[5] Briscoe, B., Odlyzko, A., & Tilly, B. (2006). Metcalfe's Law is Wrong. Retrieved from IEEE Spectrum: https://spectrum.ieee.org/computing/networks/metcalfes-law-is-wrong.
[6] M. Van Eeten, J. B. (2010). The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data. Retrieved from WEIS: http://weis2010.econinfosec.org/papers/session4/weis2010_vaneeten.pdf.

interconnectedness and placing a certain amount of responsibility onto the Internet Service Providers might help created a safer network.

Outsourcing

Given the complexities of cyberinfrastructure, it is impossible for any one player to be completely responsible for an entire process chain. Therefore, while governments provide regulations and reparation measures, the process of security itself is usually left to private actors within the realm. Network services, and software provision for example, are usually provided by private actors due to the nature and complexity of the tasks required and the proficiency of the private sector in the space. However, while outsourcing can increase efficiency through distributed work and payloads, if the actors involved in service provision are not invested or affected by an attack on the system, they will be less likely to ensure efficient and rigorous implementation of standards and norms.

While analyzing the economic aspect of information security, Dimitrios C. Koumaridis identifies certain inherent risks with the outsourcing of systems operations. These are irreversibility of decision, ability to operate new system, lack of legacy and new system integration, lack of experience managing the outsourcing relationship, excessive dependence on outsourcer, the lack of outsourcer staff experience, the outsourcer not complying with the contract, the hidden costs in outsourcing contract, unclear cost-benefit relationship, security (data confidentiality), the loss of IT expertise, and the opposition of internal staff.[7] In order to counter these difficulties, it would be helpful to build a more invested form of outsourcing with clear directions regarding the protocol to be followed in the case of breaches and attacks.

The fact remains that governments and organizations outsource a large amount of software and system development. The risks of poor software development and the lack of a liability structure in place for private actors leads to greater cybersecurity risks and higher incentives for hackers to exploit bugs and vulnerabilities. Developing streamlined outsourcing protocol should be a mandatory part of information security policies. Developing risk approaches and appetites should be an essential part of any security plan and both these approaches would need to take into account security protocol before outsourcing data, IT systems, software requirements, etc. While outsourcing is not a complete evil, and there are ways to ensure security is maintained, in the absence of liability trails, no individual party feels obligatory responsibilities for providing security. Finding ways to ensure cyber-secure software development and

[7] Koumaridis, D. (2010). Information Security Economics: An analysis for the impact of unsecure information in the enterprises. Retrieved from https://dspace.lib.uom.gr/bitstream/2159/14192/1/KoumaridisDimitrisMsc2011.pdf.

attributing responsibility in the case of a system failure/breach would be an extremely important first step in ensuring individual as well as organizational security.

Network Externalities

The interconnected nature of the IT industry proves has led to the creation of several 'externalities'. There are three key types of externalities that are posited by researchers today. These are i) network externalities, ii) externalities of insecurity and iii) interdependent security. Network Externalities refer to cases wherein "a larger network, or a larger community of software users, is more valuable to each of its members."[8] This leads to a predominant privileging of particular platforms and systems due to an overconvergence of users. For corporate systems, while features and performance would play a certain role towards the choice of platform, convenience and translatability of systems – in terms of the number of mutual users – would also play a key role in determining what platform to adopt.

The problems with such systems is that they continue to deeply entrench themselves into patterns of being and breaking out of these patterns for better security practices becomes an extremely difficult challenge. Moore and Anderson point to network externalities as key reasons for the rise of Windows, Microsoft Office, Facebook and iTunes. Furthermore, the lack of updation towards more secure internet protocols such as DNSSEC and S-BGP have also failed to achieve widespread adoption as it would require an entire network to shift platforms. While talking about DNSSEC and S-BGP, Moore and Anderson state that "Such protocols do not help much until many other users have also adopted them, so no-one wants to go first. The protocols that have succeeded such as SSH and IPSec have generally been those that provide adopting firms with internal benefits immediately."[9] The security benefits of such processes and shifts are usually hidden until a significant amount of the user database switches to the updated secure platform. This causes a deferred effect and discourages and disincentivizes early adoption.

The second type of externality - externalities of insecurity – are caused by associated risks and chain reactions. The targets of botnets, phishing mails, denial-of-service attacks are usually not the host computer from where the attack ends up being generated. The unknowing host of a 'zombie computer' within the network is just as clueless of the malware as the system that is hit. These are primarily targeted at infrastructural frameworks and there tend to be social

[8] Moore, T., & Anderson, R. (2012). Internet Security. In M. Peitz, & J. Waldfogel, The Oxford Handbook of the Digital Economy. New York: Oxford University Press.
[9] *Ibid*.

ramifications instead of private costs. As a result there tends to be a lesser amount of investment in this space which is a cause for concern. As mentioned in the earlier section, Private stakeholders – at an organizational as well as individual level – are primarily interested in safeguarding their own interests. Furthering investment towards social and public good needs to be incentivized for it to become a popular practice.

The third issue is the question of interdependent security. Kunreuther and Heal note that security investments can also be 'strategic complements'. Individuals taking protective measures may cause chain reactions and create a hygienic environment, thereby creating positive externalities for other stakeholders. The problems that emerge however, is that once a good security pattern has been established, there may be individuals or institutions that choose to 'free ride' on these incentives thereby causing a reduction in investment and leading to the re-emergence of weaker links. Information asymmetries also tie in to this aspect of the externality as the lack of cybersecurity awareness leads to callousness, thereby increasing the number and scope of vulnerabilities that can be attacked. After all, "a system is only as secure as its weakest link, and in most cases people are the weak link."[10]

Misaligned Incentives

The problem with measures towards the securitization of infrastructure as it currently exists is the lack of clarity regarding attribution, verifiability, responsibility and punishment. Furthermore, the process chain nature of most cyber-crimes can be attributed to the infrastructure and the way the internet has developed itself. One weak link within the network could be responsible for spreading malware/botnets across the entire system. In this case, the criminal is separate from the culpable target who is further separated from the eventual victims. This differentiation causes a certain alienation of the individual user from the holistic network and inevitably leads to 'convenience' being privileged over security hygiene. "Misaligned incentives occur, e.g., when the organization responsible for the security of system does not bear the full costs of its failure"[11] As Tyler Moore states in the *Economics of Cybersecurity* "Information systems are bound to fail when the person or firm responsible for protecting it does not suffer when it fails."[12] The disconnect between the authorities responsible for security and those who suffer when the security fails, is one of the key reasons

[10] Odlyzko, A. (2003). Economics, Psychology and Sociology of Security. Financial Cryptography: 7th International Conference. Springer.
[11] Lenchik, K. (2016). The Economics of Cybersecurity: Boomerang Effects from Misaligned Incentives. NTNU.
[12] Moore, T. (2010). Introducing the Economics of Cybersecurity: Principles and Policy Options. International Journal of Critical Infrastructure Protection.

de-incentivizing better security practices. Examples that Moore cites in his findings are issues of Medical Privacy, Electricity Companies, Power Grids, none of whom are held directly responsible in the case of an infrastructural failure/shutdown.

Without risk and liability allocation, developing a secure infrastructure becomes increasingly challenging. An example of this can be seen in the medical system where records are often bought by hospital directors and insurance companies, whose interests are not aligned with the needs of the patients. Another example that can be cited is the idea of Software rollouts. Oftentimes, companies will rollout software versions that are potentially unstable and develop security patches subsequently. Given the lack of attribution in the case of an exploited vulnerability there is no onus on the company providing the software to ensure stringent security evaluation. Banks and other FinTech companies also encourage their customers to use digital platforms without entirely accounting for security. Efficiency and convenience often win out over stringent security measures. The prevalence of segregated de-militarized zones should be a necessity for organizations and yet often, people will ignore these measures in order to save time and effort. These gains do not take into account the tremendous risks and vulnerabilities that emerge as a result of such negligent actions.

The lack of rigorous practices can also be extended towards the usage of un-updated security patches, converged networks, decision against operating distinct networks for distinct security protocols. This privileging of efficiency over security can also be seen in the example of network “convergence”. This refers to the fact that several critical infrastructural systems that used to operate on distinct networks, protocols and equipment no longer do so. Two key examples Moore cites are SS7 Protocols being used to manage Phone Systems and SCADA systems being used to control Electrical grids.[13] Sustaining distinct systems and protocols would require the hiring of specialized employees. Organizations increasingly began giving up on these practices in favor of training and employing engineers whose expertise was in TCP/IP and running the varying security measures and applications over common internet infrastructure. As mentioned in the case of the amount of investment necessary, however, the baseline level of specialization and segregation of network infrastructure required for minimal security needs to be found.

Another key stakeholder that is increasingly being held responsible these days are ISPs. There has been a rise in governments and regulators holding ISPs responsible for the transference of malicious traffic stemming from their domains. While ISPs have so far held onto the argument that like telephone operators they are not responsible for the traffic that passes through them, this view is

[13] *Ibid*.

increasingly changing as ISPs have a tremendous role in the digital ecosystem. Establishing a system of checks and balances using ISPs is one key way to incentivize responsible management of internet traffic and reduce spam and malware from being constantly re-proliferated. Organizations can also play an extremely important role in securing network architecture. Surveys conducted by the Centre for Strategic and international Studies (CSIS) state that cybersecurity strategies are often designed by managers and executives as opposed to operators and professionals. This changes the incentives and the method of securitization drastically as the success of security policies get measured differently. Executives would primarily be interested in ensuring minimal level investment even at the cost of lesser security. Operators who deal with breach statistics and perform penetrations and vulnerability testing on a regular basis, however, would be more in tune with the realistic security requirements. Furthermore, they would also be more aware of emergent and evolving threats as well as the recovery costs in the case of breaches and they would be able to make more informed decisions regarding the initial investment as well.

Information Asymmetries

The availability of relevant data and information is a key problem in the realm of Cybersecurity. In order to devise relevant strategies and policies it is essential to first develop a holistic map of all the vulnerabilities and breaches in the system. Doing so would not be possible unless institutions that are affected by cyberattacks come forth and provide data. There are various reasons why institutions choose to keep data and financial breaches private. These can be due to reputational costs, fear of further information disclosure, fear of driving away customers etc. What this does however, is create an environment of extreme insecurity instead. Furthermore, there is a clear imbalance between who chooses to disclose information and who doesn't. Moore states, the fact is that "we don't know the true cost of cyber-crime because relevant information is kept secret."[14] Security firms that are invested in increasing cybersecurity sales, tend to overreport incidents, while financial institutions tend to underreport incidents. The former hope that by building an environment of fear and overreporting incidents they might be able to drive up security investments, while the latter believe that reporting incidents would reduce their value, as well as have deleterious effects on the trust that they have built with consumers over the years. In other words, banks and businesses are unwilling to report information regarding breaches and are usually unwilling to work with the police on such sensitive issues as it might frighten away investors and consumers. Conversely

[14] *Ibid*.

most security companies angling to sell their products are driven towards overreporting threats and intensifying the present insecurity in the environment.

In the case of Internet Service Providers, the problem becomes even more complex as ISPs feel that the return on investments for building security strategies wouldn't match the significant investment costs. They believe that the technical costs, the legal issues, and the customer service costs would outweigh any security measures they come up with. In this case, information asymmetry plays a key role in deterring ISP security models as currently, "the information necessary (e.g., costs, pricing models) to develop a convincing business model for ISPs to provide security to their customers does not exist in the public domain."[15] A theoretical model used to describe this phenomenon is George Akerlof's theoretical model on the market for lemons. In the parable, Akerlof uses the concept of seller knowledge and consumer ignorance to prove that in a market for lemons, the market clearing price does not average out as expected as "buyers are unwilling to pay a premium for quality they cannot measure"[16] Similarly, securing a market where the buyer, or even the security provider in the ISP model, is unaware of the true risks and liabilities involved, will be impossible and the cybersecurity market will inevitable become a market for lemons.

A third key concern with regard to information asymmetries is the fear of freeloading. There are certain key paradigms of information sharing and information disclosure all of which are debated in terms of profitability of sharing within the realm of cybersecurity. Peter Swire analyses the various advantages and disadvantages associated with the same in the essay *"A model for when disclosure helps security: what is different about computer and network security?"*. [17] He analyses four key paradigms of information disclosure and the ways in which they affect cybersecurity these are:

1) <u>The open source paradigm:</u> This is based on the foundational principle that there is "no security through obscurity". It is founded on the fundamental principle that "software and network vulnerabilities, once discovered by any attacker will often quickly become known to other attackers."[18] Therefore developing an open source environment would help build better defence networks as well as encourage strategic and economically effective security strategies.

[15] Rowe, B., Wood, D., Reeves, D., & Braun, F. (2011). The Role of Internet Service Providers in Cyber Security. Institute for Homeland Security Solutions.
[16] Moore, T. (2010). Introducing the Economics of Cybersecurity: Principles and Policy Options. International Journal of Critical Infrastructure Protection.
[17] Swire, P. P. (2006). A model for when disclosure helps security: What is different about computer and network security? In M. F. Grady, & F. Parisi, The law and Economics of Cybersecurity. New York: Cambridge University Press.
[18] *Ibid*.

2) The military paradigm: Completely opposed to the Open source paradigm, the fundamental principle at play here is that given the massive amount of vulnerabilities that might exist, disclosure might actually lead to attackers learning about vulnerabilities they did not know about and yield very little for security researchers. The paradigm is founded on the belief that attackers would normally "pay a high cost to learn of the vulnerability."[19]

3) Information-Sharing paradigm: The third paradigm believes that while 'attackers may learn a lot from disclosure', so could defenders, and it is important to find a balance between information sharing and information disclosure. In other words, this paradigm is based on the belief that if information is shared within a select coterie of defenders, it reduces the risk of open access that exist in an open source paradigm. On the whole, proponents of this paradigm state that "the benefits of disclosure may be high if defenders can take additional effective measures against the attackers"[20]

4) The Public Domain: This is the final paradigm that examines the problem of information sharing and it is fundamentally based on the idea that information is always already available in some form or another. The public domain principle is founded on the idea that security experts and attackers will learn nothing new through information disclosure but that it could go a long way towards educating defenders as well as the general public. Supporters of the public domain principle also believe that "efforts to hide or reclassify information will often be expensive and not very effective in an era of the internet."[21]

On the whole while there are various reasons that need to be accounted for while examining each paradigm including 'hiddenness of attack' and 'uniqueness of defence', there are several tools such as Firewalls, Encryption, Multi Factor Authentication, all of which are aimed at creating a graded matrix of information access. Companies choose to hide information regarding security investments in the hopes that it would discourage counterparts from freeloading off of their investments as well as prevent attackers from understanding their network architecture. This is also a key reason for why companies choose to keep their breaches and the processes used secret, in the hopes of deterring further attackers while also not providing information that could help rivals secure themselves against similar threats. All this does however, is largely create a market for security redundancies, duplication, and insecurity. Furthermore, in some cases losses that can be prevented are only disclosed years later, by which

[19] *Ibid*.
[20] *Ibid*.
[21] *Ibid*.

time it is too late for most people to safeguard themselves and their information. The Equifax attack, the Uber attack and most notoriously the Yahoo attack are all key examples of how information disclosure might have helped limit the damage at an earlier stage, but instead lead to data leaks of mass proportions.

Cost of Security

The amount of money to be invested in Cybersecurity has always been a key issue at the individual, organizational as well as national level. The Gordon and Loeb model has been one of the most predominant tools for analyzing security investment. It can be traced back to a "tradition of accounting literature" and it "defines a security breach probability function which maps the monetary value of security investments to a probability of incurring a defined loss."[22] Furthermore, "[t]he GL Model provides important insights regarding the way organizations can derive the appropriate level of cybersecurity investment and the best way to allocate this investment to various information sets."[23] Recent years have also witnessed the application of Game theory to cybersecurity with researchers increasingly privileging mathematical concepts and probability to determine the scope of investment, risk and reward. While outlining a game theory model to Cybersecurity, Anna and Ladimer Nagurney provide an overview of the variations of the GL Model as developed by "Hausken who constructed different breach functions… …Matsuura, who endogenized the probability of an attack, and Tatsumi and Goto who focused on the timing of cybersecurity investments."[24] Given the complexities of information asymmetry and the relative limitations regarding the availability of data, the application of game theory and the imposition of probability and other mathematical principles onto economic and security models, is done with the intent of developing smart investment strategies and providing maximum risk at minimum cost.

Another key concern with regard to investing in security strategies is whether they should be preventive in nature or reactive in nature. Cybercrime can never be foreclosed as a possibility because finding a lone bug is much easier than fixing all the vulnerabilities that exist entirely. Given the roll out and then fix procedure adopted by most software companies, at any given time all an attacker needs to do is identify a single vulnerability while a defender has to constantly be on the lookout, fixing any and all vulnerabilities. As a result, investing solely in a preventive model of cybersecurity would leave companies woefully unprepared in

[22] Böhme, R. (2010). Security Metrics and Security Investment Models. IWSEC 2010: Advances in Information and Computer Security (pp. 10-24). Springer.
[23] Gordon, L. A., Loeb, M. P., & Zhou, L. (2016). Investing in Cybersecurity: Insights from the Gordon-Loeb Model. Journal of Information Security.
[24] Nagurney, A., & Nagurney, L. S. (2015). A Game Theory Model of Cybersecurity Investments with Information Asymmetry. Netnomics.

the even where a breach or an attack does take place. Since absolute security is impossible, it is also important to think about relative deterrents that can be adopted and the diversification of investment models necessary for developing holistic security strategies. While preventing the hack from taking place in the first place would be ideal, limiting the rewards of a hack by setting up efficient protocol regarding what needs to be done in the case of a hack is also extremely necessary. Given "the irregularity of computer software development and the evolving nature of hackers",[25] the threat spectrum can never be predicted with complete accuracy. The argument is that the "optimum level of cyber security investment is where the marginal costs of increased information security equal the marginal decrease in costs due to events such as virus attacks, hacking and break-ins"[26] and therefore any approach that attempts to achieve this balance would necessarily need to be proactive and reactive in equal measure.

[25] Dynes, S., Goetz, E., & Freeman, M. (2007). Cyber Security: Are economic incentives adequate? International Conference on Critical Infrastructure Protection. Springer.
[26] *Ibid*.