CSE H0240: Law and Policy Issues in Cybersecurity

Position Paper On
Incident Response, Incident Notification, and the Law

Created By:

MD ABDUL KADIR

Submitted To:
Professor Benjamin Dynkin & Professor Barry Dynkin
CSE H0240 Course Instructor
Department of Cybersecurity (MS Program)
Grove School of Engineering
The City College of New York

Academic Session- Spring 2023

Cyber attacks have increased in number and complexity in recent years, and companies and organizations have accordingly raised their investments in more robust infrastructure to preserve their data, assets and reputation. However, the full protection against these countless and constantly evolving threats is unattainable by the sole use of preventive measures. Therefore, to handle residual risks and contain business losses in case of an incident, firms are increasingly adopting a cyber insurance as part of their corporate risk management strategy.As a result, the cyber insurance sector - which offers to transfer the financial risks related to network and computer incidents to a third party - is rapidly growing, with recent claims that already reached a $100M dollars. However, while other insurance sectors rely on consolidated methodologies to accurately predict risks, the many peculiarities of the cyber domain resulted in carriers to often resort to qualitative approaches based on experts' opinions.

The modern society is highly dependent on Information and Communication Technologies (ICT). However, despite its paramount importance, the use of ICT also introduces a series of hazards. In fact, computer systems and services are routinely compromised and cyber incidents adversely impact many organizations, hampering business-goal achievements and resulting in copious financial losses. For this reason, cybersecurity has quickly become a subject of debate in executive boards and companies are increasingly investing in ICT security products. Overall, the security sector is expected to grow in 2019 to a 124 billion USD market, with application security testing, data loss prevention, and advanced threat protection representing the core investments.

Despite the importance of this considerable and rapidly-increasing effort, it is well understood that cyber attacks cannot be prevented by technical solutions alone and the protection against all possible threats is neither possible nor economically feasible. Thus, in order to handle the residual risk, organizations are rapidly moving towards managing their cyber risk by incorporating cyber insurance into their multi-layer security frameworks. Cyber insurance is defined to be the way to transfer the financial risks related to network and computer incidents to a third party. Compared with traditional insurance policies for business interruption and crime, a cyber-insurance policy can also cover, for instance, digital data loss, damage and theft, as well as losses due to network outages, computer failures, and website defacements.

While researchers and security experts are still debating whether cyber insurances even make sense and how they could be better implemented, insurance companies are already selling them as part of their portfolio. We may like it or not, but this is already a reality and as it often happens in our field, security needs to catch up with an immature technology that was rushed to the market.Companies are currently struggling against the demand of cyber policies as existing tools and methodologies to assess risk exposures and pricing are inadequate in the cyber domain.Without considering catastrophic scenarios, the vast majority of cyber risks are insurable, carriers are missing solid methodologies, standards, and tools to carry out their measurements.

Insurance is a risk management method whose main purpose is to convert the risk of harmful events into an expenditure. The insurance process generally involves two players: a first supply-side entity who provides insurance, named insurer or insurance company, and a second demand-side entity who buys the insurance, known as insured or policyholder. The two parties interact in two different phases, respectively identified as underwriting (or policy stipulation) and claiming for compensation. During the drafting of a policy, an insurance carrier needs to acquire useful information about the prospective client with the purpose of identifying his risk class. Afterwards, the two parties need to clearly define the conditions, circumstances, and nature of the events that are covered by the policy. Coverage can encompass both first- and third-party losses: while the former is purchased to cover the policyholder against damages or losses suffered by the insured to his person or property (e.g., health, disability insurance), the latter is intended to protect the policyholder against liability for damages or losses caused by the insured to other people or their property (e.g., bystanders hit by insured's car in an accident, stranger's properties damaged by a fire that comes out of insured's house). At this point, the insurer quantifies the material damage that the insured — or third subjects if considered — would be subjected to if these occurrences were to happen. Finally, the insurance company takes on the liability and management of such situations cashing a premium payout from the insured.

Factors Affecting the Development of a Cybersecurity Culture

The following are some of the factors which influence the development of a cybersecurity culture:

a) Clarity of Policies

For the cybersecurity culture to be effective, it is paramount for the organization's management to create policies which clearly address the potential threats in the immediate working environment, the available preventive measures and how to respond in case a potential or actual attack has been detected.

b) Assumptions Made by Management Members

The assumptions made by policy makers with regard to the roles played by different people in the culture development process could determine whether the culture becomes effective or not.

c) Points of Focus for Policy Makers

In the development of a cybersecurity culture, the main aim of cybersecurity policies is to condition people within the organization into doing what is required so as to safeguard data integrity.

d) Communication Development Efforts

The efficiency of communication determines whether the policies will be perceived as laws which they must comply with or a culture which needs to be cultivated for the greater good of the organization. A main component of organizational culture and managerial culture is managerial communication. Employee' satisfaction and commitment is defined by the organizational culture .Welch and Jackson concentrate on the fourth dimension which is the internal corporate communication. The main role of this type of communication is to "transfer" the goals and the objectives of the organization and aims to reach four goals: the understanding of the business environment, the belonging, the commitment and the awareness.

e) Cooperation Development Efforts

Cooperation is a basic component in order to aggregate activities, as well as to keep up a beneficial general workplace. The business workplace groups showing lack of teamwork may lead to unwanted results at business operations. For every stakeholder to play their role in cultivating a cybersecurity culture, they must understand the dire importance of their role as well as the ultimate collective goal.

f) Csirt's Effectiveness Improvement

Bada et al. argued that the measurement of the effectiveness of information security will assist in increasing accountability, improving the effectiveness of information security, as well as the demonstration of compliance. The researchers also argue that in order to improve the effectiveness of CSIRTs, relevant information issues such as trust, data-sharing, better communication and cooperation are necessary to be explored, which are important in achieving the highest levels of performance.