A Statistical Study on A New Era of Information Security and Cyber Risk Management: Cyber Insurance

Shreyas Pathak[1] Shiny Khajuria[2]
[1,2]Student
[1]Department of Electronics & Communication Engineering [2]Department of Computer Science & IT
[1]Gujarat Technological University, Ahmedabad, India [2]University of Jammu, Jammu, India

Abstract— Have you ever imagine a bank without security or even lockers? With the prompt extension of the information age, electronic movements of many kinds are becoming more common now days. Recent work in security has illustrated security attacks are unlikely to result in robust cyberspace. With the increasing cost and volume of data breaches, cyber security is quickly moving from being considered by business leaders as a purely technical issue to a larger business risk. This analysis will also discuss the barriers that hamper cyber insurance's development into a mature market. Lastly, this paper will illustrate the prospective for collaboration between the private sector and academia and suggest a research agenda for the setting of cyber insurance policy premiums.

Key words: data breaches, cyber insurance, CLIC, styling

I. INTRODUCTION

A frequent answer from, security professionals have been saying "either you have been data breached or you just do not know that you have been data breached". Data breaches are now a fact of life together with taxes and death, but how can businesses better manage the risks related to a data breach and reduce the significant cost that can result from them? One of the available options is to buy insurance. Cyber liability insurance cover (CLIC) has been available in the market since 10 years, although most security professionals seem unlikely to have heard weather is exists or not. CLIC has been most well-to does used as a risk transfer option in those countries that have compulsory data breach notification laws.

The best example of this is the United States, where 46 of the 50 states have mandatory requirements for data breach warning. In the UK, the imminent draft EU Data Protection Regulation incorporates compulsory notification of breaches, but the scale and timing of this new regulation is still to be resolute.

II. PROBLEM IDENTIFICATION

Current technologies have aid to grow effectiveness and productivity and have also created new business prototypes. Nevertheless, there is no contradicting that they have also created new threats to companies. Cyber attacks can have a devastating impact on a company: a study found that the average financial impact of a cyber attack was $9.4 million and that future attacks could potentially result in costs as high as $163 million. As the market for e-commerce alone was valued at $7 trillion back in 2005, there is great potential for more costly attacks. Thus, companies have to come up with responsive ways of dealing with cyber ambush. Similar to other risk management areas there are three basic strategies: self-protection, self-insurance, and transfer of risk through (cyber) insurance[4].

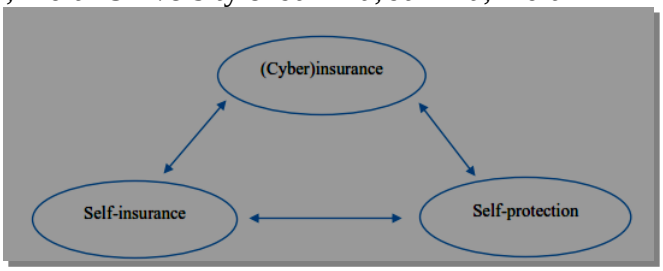

Fig. 1: Policy to deal with Cyber-risk

As Figure 1 shows those strategies offer discrete ways of dealing with the risk of cyber attacks but can also work together in a mix. *Self-protection* refers to investments made to lower the risk of an attack such as IT security infrastructure, policies, e.g. encryption, and raising awareness among employees. However, investment in self-protection measures has been found to be too low and ill-conceived, leading to sometimes perverse incentives, e.g. bad configuration of otherwise useful systems. Self-protection also includes so-called 'active defenses', where a company that has fallen victim to a cyber attacks takes active steps against a perpetrator, e.g. "hacking back"[2]. Under the current legal framework such steps are, discouraged and it is far from clear that such measures will work[7].

A consensus is growing that IT security is not achievable by solely focusing on technological aspects. The present risk of cyber attacks is "essentially a business problem"[1].Hence, in addition to lowering the likelihood of cyber attacks through mostly technical means, companies can try to absorb losses incurred by such attacks through *self-insurance*, i.e. setting aside funds. Of course, this would necessitate the ability to judge and adequately quantify the risks and the availability of sufficient resources. Depending on the size and capabilities of the company, this might prove difficult or even impossible. Finally, the risk can also be transferred through a specific *cyber insurance* policy. In that case, the insurer agrees to bear the losses incurred by cyber attacks and receives a recurring policy premium in return. Companies need to understand the extent of their current coverage and identify possible vulnerabilities in order to choose an adequate cyber insurance policy.[23]

Ideally, companies deal with the risk of cyber attacks by using a combination of the above mentioned methods.[24]But how do managers make their choices about how much they should invest and in what strategy? First, managers need facts about the risk of cyber attacks and the three possible mitigation strategies. Second, based on those facts and the incentives they face, managers will make a decision. To appeal to "business people," people in charge of IT have to translate the risks of cyber attacks into numbers and provide objective information instead of the common "fear, uncertainty and doubt" tactic. One measure of doing so is to provide a return on security investment (ROSI).[26]This measure takes into account that "security is

not usually an investment that provides profit but loss prevention" and helps companies to answer such questions as: are we paying too much for our security? Is a specific security product/service beneficial? However, ROSI is not without its critics[4].

The next step of decision-making investigates what incentives exist for individual companies to invest in one or all of the strategies. This is called the economic approach to information security. We can understand risk mitigation of cyber attacks as a market - actors can invest in certain strategies to protect against attacks from other actors[5].Within this framework of economic analysis we can assess the impact of different choices, e.g. what happens when companies get together and collaborate in the field of IT security or what influence new government regulations, e.g. to disclose information about cyber attacks, have on the incentives of individual companies to invest in the security strategies[6].

Focusing on incentives reveals not only options for companies, but also what role the government can play by changing those incentives, e.g. through new regulation[4]. However, governmental changes to the incentives can also create their own problems[8].Insurance can provide for a market-based way of changing incentives towards more adequate security investment[9].Hence, cyber insurance is not only an interesting addition to the basket of mitigation strategies from a company's perspective, it is also interesting from a societal perspective, as it might improve the overall IT security.

III. METHODOLOGY

Data breaches are now facts of life together with taxes and death. With the rise in data breach incidents and impending legislation, this is all going to change.

Fig. 2: CLIC affected services

A. CLIC (Cyber Liablility Insurance Cover):

The term "cyber liability insurance cover" is often used to describe a range of covers - in very much the same way that the word cyber is used to describe a broad range of information security related tools, processes and services.

At the moment, cyber liability insurance cover can include;

- Data breach/privacy crisis management cover. For example, expenses related to the management of an incident, the investigation, the remediation, data subject notification, call management, credit checking for data subjects, legal costs, court attendance and regulatory fines.
- Multimedia/Media liability cover. Third-party damages covered can include specific defacement of website and intellectual property rights infringement.
- Extortion liability cover. Typically, losses due to a threat of extortion, professional fees related to dealing with the extortion.
- Network security liability. Third-party damages as a result of denial of access, costs related to data on third-party suppliers and costs related to the theft of data on third-party systems.

Some of the elements of a cyber liability cover may be interconnected or overlap with cover from existing products, including those for business continuity, third-party supply chain issues and professional indemnity. Even if this overlap does exist, a decent cyber liability policy will ensure cyber risks are fully catered for.

B. Ridge Methodology:

(1) Inform with real cyber intelligence: Utilize world-class cyber intelligence capabilities to illuminate specific company and sector threats, not just general risk, across the global cyber domain.

Fig. 3: Cyber Intelligence

(2) Assess specific client risks: Leverage the intelligence to deliver a client-focused, informed assessment that assists both the insured and insurer in recognizing true disruptive cyber business risk—avoiding a "check-the-box" approach that is too often standard.

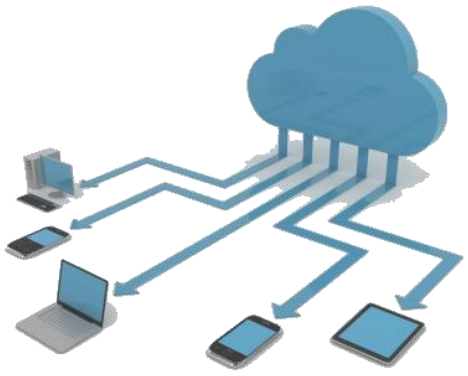

Fig. 4: Cyber risk in Cloud

(3) Act to reduce risks and rates: Utilize the information from the intelligence and assessment phases to take mitigating action which may reduce client cyber risk exposures and insurance premiums.

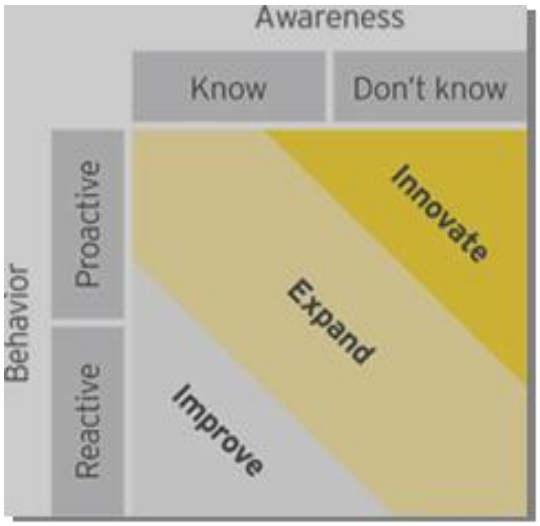

Fig. 5: Strategy to reduce Cyber Risk

IV. Evolution and Market Challenges

While there is disagreement about the exact birth date of cyber insurance policies, it is clear that the market is relatively new and not yet mature[5].Considering the potential benefits of cyber insurance as outlined above, the first cyber insurance policies sparked hopes that "cyber insurance might become as important and as ubiquitous in the IT security toolbox as firewalls and antivirus software." Government officials also praised cyber insurance as an important mechanism to increase IT security. However, the growth of the cyber insurance market has somewhat been tentative and slow, prompting experts to revise their initial forecasts for the evolution of the market[6]. Inadequate coverage by "traditional" policies, increased vulnerability, and exposure to cyber risks (as well as lack of resources to self-insure) should be driving the demand for cyber insurance policies. Until recently, few companies planned to buy cyber insurance policies and an even fewer number actually bought cyber insurance policies. Still, the market for cyber insurance policies is here to stay and expected to grow in the future.

Fig. 6: Graph showing percentage of Cyber Insurance purchaser

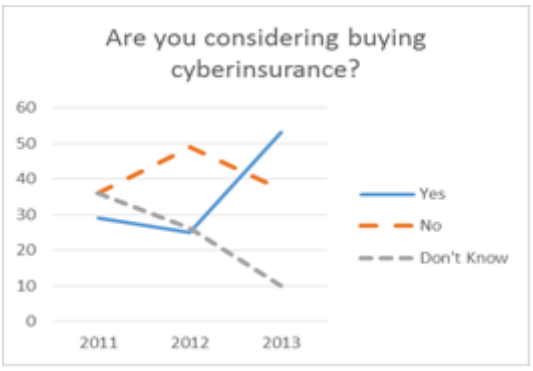

Fig. 7: Graph showing percentage of Cyber Insurance is required

Parameters	Travlers	Chubb	Philadelphia
Network Security & Info Liability	Network & Information Security Liability	Cyber Liability	Network Security & Privacy Liability
Regulatory Defense Expenses	[same]	Cyber Liability	Privacy Regulations
Errors & Omissions & Wrongful acts	Technology Errors & Omissions	Integrity+	Network Security & Privacy Liability / E&O
Communication & Media Liability	[same]	Cyber Liability	Electronic Media Liability

Table 1: Cyber insurance in worldwide business organizations

The latest trends seem to support this optimistic view: A recent Adviser report identified 2013 as a possible "cyber tipping-point," stating that after large firms were mostly aware of their risk exposure to cyber attacks, "smaller businesses began to increasingly realize that they were also at risk." This reflects that "insurance [had] cemented itself as a part of the cyber risk management strategy for a majority of companies surveyed by Adviser."[50]In line with these findings, a Ponemon Institute report showed that companies are concerned about future cyber attacks. This is likely to drive demand for cyber insurance further in the future.[51]

As Figure 7 shows, more companies are not only considering to buy cyber insurance - they are buying policies. This is moving cyber insurance "into the mainstream as a tool for managing IT security risks."

V. Conclusion

Think of cyber insurance as another part of maintaining the security of your digital assets. Years ago, you began this process when you first licensed firewall software and subscribed to an antivirus service. Since then, as the IT side of your organization has become more complex, you have been doing what you could to keep sensitive capabilities and information secure. Maybe you have installed a virtual private network (VPN), use public-key encryption, digital

certificates, and digital signatures. Perhaps you have retained the services of a cyber security expert. Ultimately, the value of your organization is the information you possess. Protecting it is a never-ending process. Villains will always be striving to stay one step ahead of those who would thwart their malicious actions. Cyber insurance extends your wall of security one level further.

REFERENCES

[1] Advisen. "2013 Information Security Cyber Liability \& Risk Management." Tech. rep., Advisen
[2] Anderson, Roberta D. "Insurance Coverage for Cyber Attacks - Part One of a Two-Part Article."The Insurance Coverage Law Bulletin 12, no. 4 (2013).
[3] Bandyopadhyay, Tridib, Vijay S. Mookerjee, and Ram C. Rao. "Why IT Managers Don't Go for Cyber-Insurance Products." Communications of the ACM 52, no. 11 (2009): 68-73.
[4] Capgemini. "Using Insurance to Mitigate Cybercrime Risk." Tech. rep., Capgemini, 2012.
[5] Daniel, Michael. "Incentives to Support Adoption of the Cybersecurity Framework." Incentives to Support Adoption of the Cybersecurity Framework. http://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity, framework ,August 2013.
[6] Friedman, Allan. "Economic and Policy Framework for Cybersecurity Risks." Center for Technology Innovation at Brookings July (2011): 1-24.
[7] HBR. "Meeting the Cyber Risk Challenge." Tech. rep., Harvard Business Review Analytic Services, 2013.
[8] Ponemon. "Manaing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age." Tech. rep., Ponemon Institute LLC, 2013.
[9] Schneier, Bruce. "Hacking the Business Climate for Network Security." IEEE Computer April (2004): 87-89.

