How to Dynamically Incentivize Sufficient Level of IoT Security

Abstract. This paper propose an incentive mechanism to make large number of device secure based on insurance by smart contracts. It consists of the automated security evaluation of enterprise IoT devices and the creation of a dynamic insurance premium. To automate the security evaluation of enterprise IoT devices, we collect and store IoT device status data with privacy preservation on blockchain. Then, we track and assess the risk associated with IoT devices with the use of a smart contract. By monitoring this risk over time, we present a means to incentivize the resolution of vulnerabilities by judging the latent risk in an environment as well as the vigilance of the devices' managers in resolving these vulnerabilities. In this way, we produce a dynamic cyber insurance premium that more accurately captures the risk profile associated with an environment than existing cyber insurance. Through the use blockchain and smart contracts, this framework also provides public verification for both insured and insurer and provides a level of risk management for the insurer. We also present regulatory considerations in order for this scheme to meet supervisory requirements.

Keywords: Smart Contract, Blockchain, Cyber Insurance, Privacy Preservation, Regulation Awareness

1 Introduction

1.1 Background

Smart contracts are a mechanism originally proposed by Nick Szabo to process business logic autonomously. The automation of business processes provides increased benefits to large-scale systems with multiple stakeholders as it eliminates many negotiations between stakeholders. The implementation of this concept necessitates a shared place to record and update a common data set. Blockchain technology is a significant breakthrough to realize such a distributed ledger that was originally developed as part of Bitcoin. Blockchain forms the foundation of smart contracts between any number of stakeholders and allows the development of smart contract platforms such as Ethereum. In a similar manner to crytoassets as an application of blockchain technology, the use of smart contracts has garnered the attention of the financial industry. A large number of experimental proof-of-concept systems have been built upon smart contract platforms. Insurance is one of promising application area of smart contract because it consists of different types of stakeholders such as insurance companies, insurers, insured persons/corporations, and auditor. This business requires negotiation in deciding the insurance fee at the time of contract, and deciding amount of money

of actual payment at the time of accident. Automating such processes for huge numbers of stakeholders is required.

As an example of a target of such an insurance product, there is the cyber security of huge numbers of devices that are essential to our life. Since first becoming practical to produce, market, and distribute inexpensive internet-connected appliances, the realm of "Internet of Things" has grown immensely. In almost all instances, there is a stark lack of attention paid to the security of these devices. Usually, security incidents occur by attacks on the weakest link of the system. Nowadays, most devices have functionality such as an update mechanism to apply security patch, however, the application of the security patch cannot be automated because it may inject another bugs and vulnerabilities. In practice, it takes more time to apply the security patch than expected there may be additional security risks. In the worst case scenario, the entity completely neglects to update some of the devices they manages. Properly securing Internet of Things (IoT) devices involves identifying the presence of compromised devices on a network as well as tracking and resolving the risk they present. In the era of IoT, the task to manage all devices in a system to be updated from security viewpoint is becoming increasingly difficult, and sometimes it becomes an impossible mission, though people expect the system to operate securely. To resolve this issues, we need an automated system to help humans manage the huge amount of devices and provide them sufficient incentives to make their own devices securely updated.

1.2 Related Works

Since we cannot assure 100% security for any system, designing insurance for cyber security is an essential building block to ensure secure and safe use of the system. There are a large number of existing research works on cyber insurance. Sasha and *et al.* [11] answered fundamental questions of cyber insurance such as how insurance carriers write insurance policies and calculate premium in their paper. In [12], Danial and *et al.* have proved that cyber insurance will promote security best practice. While questions remain regarding how cyber insurance as a means of transferring cyber risk could provide incentives of proper adoption of security controls over time. Several authors [2,14] have indicated that insured party takes several security controls required by insurance carrier in return for reduced premium. However, the premium discount is applied at the beginning when an insurance contract is signed and insurers can not track and evaluate security postures of insured party. Continuous incentives of the adoption of security controls are necessary.

There are several proof-of-concept level trials on this direction. Existing work on cyber insurance involving smart contracts and high resolution data in general maintains a distinct scope from our focus on dynamic pricing. For example, the Smart Contract Insurance project from ASU Blockchain Research [7] focuses primarily on the automating the negotiation of settlements based on predefined triggers and the Smart Cyber Excess Insurance from Corvus [5] which uses data

to aid the underwriting process but not to create a fully dynamic insurance premium.

There are existing discussions about regulatory implication on applying smart contract to financial services and products in general such as Finck [4]. However, as far as we investigate, there is no academic discussion on the in-depth regulation issues on the cyber insurance based on smart contract.

1.3 Contributions

In this paper, we offer an approach as to how one can increase the security level of IoT devices with sufficient incentives by using smart cyber insurance. The inclusion of dynamic pricing mechanism creates incentives for the proactive patching and resolution of security vulnerabilities. When compared to penetration testing and other in-depth surveys that are performed annually, our proposal dramatically reduces the cost of obtaining high-resolution vulnerability information about a insured client's environment. Other methods of obtaining this information only represent the state of a insured client's environment at a given time and cannot quantify the vigilance or responsiveness of an insured company when new vulnerabilities are discovered. In addition, we identify key considerations on how our scheme can meet regulatory requirements.

2 Smart Insurance for Cyber Security

2.1 Overview of Cyber Insurance

Thousands of data breaches and security incidents occur each year and cost hundreds of millions of dollars. To mitigate these losses, organizations and companies turn to cyber insurance to transfer their risk to the insurer. Insured organizations benefit from this risk protection while insurers profit from premiums. Insurers can also encourage increased security investments from companies and organizations by sharing information regarding cyber-attacks and offering premium discounts for applicants that adopt security controls dictated by the insurer [13]. As a result, cyber insurance drives improvements in cyber security. In general, cyber insurance is for covering risks in the real operation of a system. ISO/IEC TR27103 [1] describes a framework of such operation. Cyber insurance is thought to cover risks in this framework. Such risks are caused by many factors such as costs, liability and loss by business interruption. Most of existing cyber insurance products try to cover such risks, but they do not cover everything, e.g. penalty against data breach regulated by GDPR. Factors are categorized into two: technical and human factor. This paper concentrates on the technical factor.

2.2 Challenges of Cyber Insurance

2.2.1 Soundness

The soundness of cyber insurance is indicated by five aspects:

- Insurance contract is based on the agreement of stakeholders.
- Agreed contract cannot be altered.
- Insurance premium and claim should be in accordance with signed contract.
- Insured party cannot obtain more insurance coverage than the defined coverage in the original contract.
- Insurance carrier cannot pay lower coverage to insured party than the defined coverage in the original contract.

2.2.2 Privacy

The insured party must be able to provide information about their security status in a manner that does not compromise their system's integrity or significantly confide in another party. It is undesirable for a party with vulnerabilities to broadcast this information. Therefore, the sharing of the high resolution information that enables the dynamic nature of the cyber insurance scheme must be protected from unknown external parties. Similarly, it is crucial for the insured party to share the minimum level of detail that is required by the insurer to implement such a dynamic system. There exists an optimal level of detail that is a balance between providing high resolution dynamic information to the insurer while simultaneously limiting the scope of this information in order to protect the insured party.

2.2.3 Difficulties of Existing Cyber Insurance Business

Despite increasing demand, the cyber insurance market still account for less than one percent of total U.S. insurance premiums. According to EIOPA [6], even existing cyber insurance shows a low conversion rate. This implies that the cyber insurance products do not meet policyholders needs and/or policyholders do not have insufficient level of understanding of the products. In a conventional cyber insurance scheme, the insurance premium is based on simple surveys, industry evaluations, and the level of coverage. This analysis is static and only reevaluated on renewal of the insurance contract.

EU-U.S. Insurance Dialogue Project [10] stated several obstacles that insurers have been facing. One of the biggest problems is lack of historical claims data and resulting weak risk modelling, which makes adequate pricing difficult. It is mainly due to lack of reporting and relatively new, complex and changing nature of cyber risk. Though some insurers make efforts to gather data from external providers, difficulties are observed in collecting sufficient amount of data of advanced systems and measuring the relevance to the current or future cyber landscape. In consequence, majority of existing insurance products rely on insufficient qualitative model and do not provide incentives for policyholders to proactively secure their network environment. In this regard, a scheme which has quantitative modelling and proper incentive mechanism could play a important role in improving cyber insurance business.

2.2.4 Regulation

Insurance regulators are paying increasing attention to the risks associated with underwriting cyber insurance as the market expands[1]. In the U.S., for example, all registered insurance companies who write cyber insurance are required to report associated data such as direct premiums written and earned to the National Association of Insurance Commissioners (NAIC) [8]. State regulators use this data to review how insurers set prices and policy terms for new cyber insurance business in order to confirm that the insurer properly understands and controls the risk.

Regulators have taken several steps to identify key challenges and improve supervisory practices. According to EIOPA [6], there is a need for both insurers and policyholders to deepen their understanding of cyber risk to support better underwriting and purchasing decisions. Some insurers underwrite cyber risk without the use of any modeling while policyholders choose insurance by price rather than the assessment of indemnity. Aggregation risk is another concern as the increase in connectivity of IoT devices could cause unexpected insurance loss in distressed situations where catastrophic cyber incidents break out on a global scale. In addition, IAIS [9] pointed out that insurers are prime targets for cyber criminals who seek information that later can be used for financial gain through extortion, identity theft, or other criminal activities.

In this regard, the smart cyber insurance scheme can play a positive role in aspects such as sophisticating underwriting practices of cyber insurance and mitigating the concentrated risk of sensitive information. However, given the relatively complex nature of the scheme and the limited expertise of examiners with blockchain technology, smart cyber insurance products are likely to be thoroughly reviewed in many jurisdictions to confirm their positive or negative impact on an insurer's business, financial stability, and policyholder protection.

2.3 Dynamic Pricing and Incentive Mechanism

To address the challenges discussed in section 2.2, we introduce a dynamic pricing mecanism to cyber insurance based on smart contracts. Using smart contracts in cyber insurance provides transparency between the insurer and the insured, allowing for increased efficiency in the insurance marketplace by removing the asymmetrical knowledge of an insured organization's vulnerabilities. Allowing insurance companies more transparency into the insured party's Internet of Things ecosystem permits more accurate, and potentially lower, insurance premiums for the insured party.

The smart insurance scheme also records the responsiveness of an insured party to vulnerabilities that have been discovered in their environment. The time taken to address vulnerabilities is then factored into the calculation of an insured party's insurance premium. In conjunction with the increased transparency provided to the insurance company, this time-scaled insurance scheme

[1] U.S. direct premiums written for cyber risk coverage were approximately 2.03 billion dollars in 2018, a 10 percent increase over 2017's 1.84 billion

can be adapted to provide dynamic insurance pricing to an insured organization. Since the smart insurance scheme is informed of the state of an insured system's security, updated insurance contracts can be created on any interval the insured party and insurance provider agree on, even hourly or daily. Compared to offering premium discounts to incentivize security postures of insureds, this dynamic insurance scheme provides a more clear financial incentive for an insured party to proactively secure their network environment, resulting in lower premiums for the insured party and lower risk for the insurance provider. Depending on the vulnerabilities encountered, this scheme may help avoid the widespread use of botnets and increase the overall security of the Internet.

3 System Design for Smart Cyber Insurance

3.1 Stakeholders

Stakeholders of smart cyber insurance system consist of:

- Security organizations and security vendors
  Security organizations and security vendors provide security information and patch to end user and make a profit.
- Business entities, individuals and IoT devices
  Business entities, individuals and IoT devices protect their own privacy or their custom's privacy to minimize expenses of any single breach.
- Insurance companies
  Insurance companies provide accurate cyber insurance policy and make a profit through their insurance product.
- Manufactures and application developers
  Manufacturers and developers provide hardware and software products.

3.2 System Model

The smart cyber insurance system consists of vulnerability information management, IoT device status management, and cyber insurance management. The security information management platform allows NIST and other security organizations to publish security and vulnerability information and allows other entities in the network to access published security and vulnerability information. The IoT device status management platform allows individuals or the IoT device manager to record encrypted installed-software data and allows the insurance company to access that encrypted data. Insurance management allows the insurance company to manage cyber insurance policies of the insured party, and allows the insured party to access their insurance policies.

The primary components of a smart cyber insurance system are a blockchain to store the installed software database, a vulnerability database populated with information published by NIST, smart contracts for interacting with the blockchain, an application local to the IoT devices for vulnerability detection, risk score calculation, and the insurance premium and coverage calculation. The primary components and stakeholders of the system are illustrated in Figure 1.

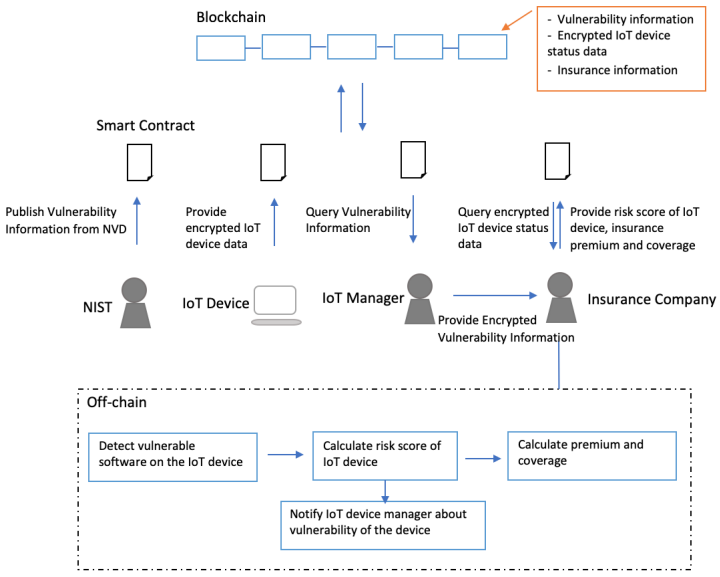

Fig. 1. System model of smart cyber insurance

3.3 Detailed Process

The system functions such that a security organization such as NIST publishes vulnerability information from national vulnerability database (NVD) to blockchain. Each entry of vulnerability information includes CVE ID, affected product information, impact metrics, and timestamp. Examples of vulnerability information are illustrated in Table 1. Each IoT device will provide a list of its installed-software records. Each record includes device ID, vendor name, product name, version value, current risk score of device, and timestamp. Examples of installed-software records are illustrated in Table 2. To protect the privacy of the IoT device, records of installed-software will be encrypted before they are stored on blockchain. The IoT manager will store encrypted IoT device status data also known as encryption of installed-software records to the blockchain and provide proper tokens of vulnerability information to the insurance company. The insurance company will use those tokens and encrypted IoT device status data from the blockchain to measure a device's risk level and calculate its risk score. At the end, the insurance company will use risk scores of all insured IoT devices as an input of insurance model to calculate premium as well as coverage. We describe details of two triggers of the system in the following paragraphs.

In one scenario, the security organization publishes a vulnerable software such as first entry in Table 1 to the blockchain. The IoT device manager notices this event and generates a token of vendor name, product name, version value, and impact score of the entry and send it to the insurance company. The insur-

CVE ID	Vendor Name	Product Name	Version Value	Impact Score	Publish Time
CVE-2019-1	debian	debian_linux	8.0	5.9	08/01/2019
CVE-2019-2	libexpat	expat	1.95.1	3.6	08/02/2019
CVE-2019-2	google	android	4.4.4	3.6	08/02/2019

Table 1. Examples of vulnerability information

Device ID	Vendor Name	Product Name	Version Value	Current Risk Score	Install Time
1	debian	debian_linux	8.0	0	08/01/2019
1	google	android	4.4.4	5.9	08/02/2019
2	libexpat	expat	1.95.1	2.8	08/01/2019

Table 2. Examples of installed-software record of IoT device

ance company searches this token over encrypted IoT device status data from blockchain and stores it to a local database also known as vulnerability database for future use. If a match is detected, the insurance company will recalculate the risk score of the vulnerable device and write it to the blockchain. Note that for every new vulnerable software the insurance company needs a new token. Each token is unique and it is issued for a specific vulnerable software. With updated risk score, the insurance company uses the insurance module to calculate new premium and coverage and writes this information to the blockchain as part of the insurance policy for insured party.

In the other scenario, a new software is installed on insured party's IoT device and the encryption of the software information is stored on the blockchain. To measure the latest risk level of the IoT device, the insurance company scans all tokens from local vulnerability database and check if a match with the encryption of the software is existed. If the newly installed-software is vulnerable, the insurance company will update the risk score of the device and update premium and coverage of the insured party and writes them to the blockchain.

3.4 Privacy Protection

3.4.1 Requirement

There are two types of data in this system that require privacy protection: the IoT device installed software information and the cyber insurance policy information. The installed software information of the IoT devices is used in vulnerability detection, a process of scanning and comparing the databases of installed software and security vulnerabilities to find vulnerable software on the IoT devices. Only the insured party who manages IoT devices has access to their device installed software data. As for information of each insurance policy, they should be only available to the insurer and its insured party. Since installed software data and cyber insurance policy data are stored on blockchain for public verification, providing each stakeholder with proper access to those data is critical.

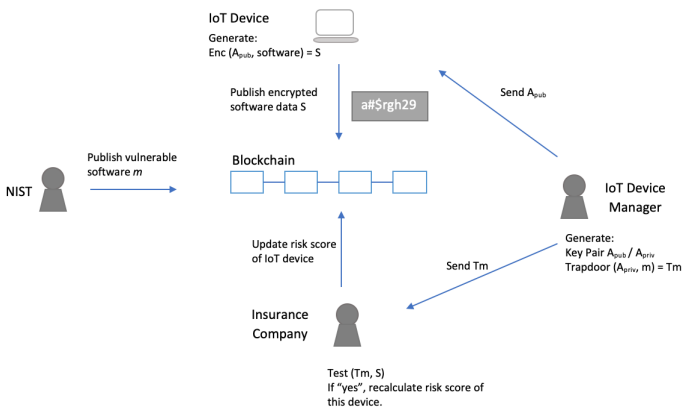

Fig. 2. PEKS in smart cyber insurance system

3.4.2 Realization Using PEKS

PEKS (Public Key Encryption with Keyword Search) is a public key encryption scheme which enables parties to search over encrypted data without revealing any additional information about the plaintexts. PEKS was first introduced by Boneh *et al.* [3] and consists of four algorithms: KeyGen, Enc, Trapdoor, Test.

- KeyGen: It generates public key pk and private key sk.
- Enc: It takes public key pk and keyword m as inputs and outputs encrypted keyword c.
- Trapdoor: It takes private key sk and keyword m' as inputs and generates a trapdoor td for keyword m'.
- Test: It takes trapdoor td and encrypted keyword c corresponding to keyword m as inputs and outputs 'yes' if td is the trapdoor for keyword m, otherwise it outputs 'no'.

In this paper, the use of PEKS enables insurance company to detect vulnerable software on IoT devices without exposing any data, including software data on the IoT devices. In other words, the insurance company is provided a trapdoor for each vulnerability and searches the encrypted IoT device data and only learns whether or not the IoT device has the specific vulnerability or not. THe use of PEKS in the smart cyber insurance system is illustrated in Figure 2 and details are as follows:

1. KeyGen: IoT devices manager of the company generates a A_{pub}/A_{priv} key pair for all IoT devices from the company. Where Apub is company's public key and Apriv is company's private key.
2. Enc(A_{pub}, software): Each installed software data on IoT device is encrypted by using PEKS scheme with A_{pub}. Then it is stored on blockchain through smart contract.

3. Trapdoor(A_{pub}, m): When security organization publishes security information m on blockchain, IoT devices manager will listen to this event and fetch m from blockchain through smart contract. Then IoT devices manager uses A_{priv} to generate a trapdoor T_m and sends T_m to insurance company.
4. Test(S, T_m): Given the encryption S = Enc(A_{pub} , software) from blockchain and T_m, insurance company could test if installed software data of IoT device matches with the vulnerable software data. If 'yes', insurance company will recalculate risk score of the device.

3.5 Risk Rating Scheme

3.5.1 Basic Summation

A naive Smart Insurance risk rating scheme would simply count the current risk based on the vulnerabilities present on the devices in a network at a given time. Although this is a functional approach to determining the security of a network at a given time, this count does not truly reflect the insured party's risk over time nor the insured party's responsiveness to these risks.

3.5.2 Time Scaling

Risk can be thought of as "having a vulnerability over time". Therefore, if you can incentivize the timely resolution of vulnerabilities, you can decrease the risk to both the insured company and the insurer. In order to develop these incentives, the risk rating scheme increases impact of a vulnerability the longer it is left unattended. By reducing the amount of time each vulnerability is present, the insured party can reduce their overall risk score. This system also allows a vigilant party to prevent a single vulnerability from significantly impacting their overall risk score and their insurance premium.

Parameters:

- I = Interval of relevance: This is the interval from which we care about counting risk scores of vulnerabilities. For example, some number of months.
- C = Score reduction time constant: Exponential functions have the feature of scaling to a limit. Using a time constant to divide the exponent, we can set how quickly this diminishing occurs.
- Δt = The time period of vulnerability: this is the interval of time between when a vulnerability is detected on a client's system and the time when they have resolved it.
- Sampling interval: The interval in which the smart insurance system receives new information. This is the highest resolution time period in which we can measure vulnerability resolutions.

Calculation:

1. Δt = (time of vulnerability resolution)− (time of vulnerability detection)

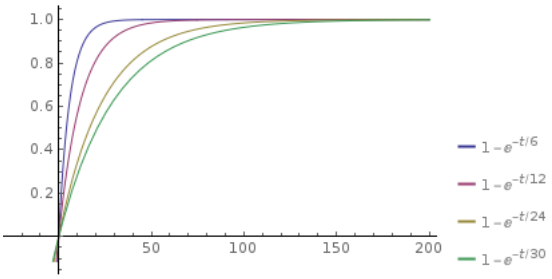

Fig. 3. Examples for various values for C

2. C =choice of time constant to shape the scaling
3. Individual vulnerability risk = (raw impact score from the security organization)× $(1 - e^{\Delta t/C})$
4. Risk score = sum of all individual vulnerability risks in the interval of interest

4 Implementation and Evaluation

4.1 Implementation Using Ethereum

The smart cyber insurance system implementation consists of two smart contracts and several java classes. We implemented smart contracts in Solidity and deployed them on a private Ethereum blockchain. The security management smart contract (SIManagement.sol) provides functions for storing vulnerability data to blockchain and retreiving that data from blockchain. The IoT device management smart contract (IoTManagement.sol) provides functions for storing the encrypted installed software data to the blockchain and for retrieving this data from the blockchain.

We implemented primary components of the system following the design described in section 3 in Java. First, we implemented the functions of PEKS. Then we implemented functions to set up connection with remote Ethereum node, load credentials, and shut down the connection for each stakeholder. In addition, we implemented java wrapper of smart contracts and specific functions for each stakeholder such as functions for insurance company to scan encrypt installed software data and trapdoor of vulnerable software and calculate risk score of IoT devices.

4.2 Evaluation

4.2.1 Soundness

Since insured party first signs insurance contract with insurer and then the contract is stored on blockchain, any part such as premium, coverage and claim of

signed insurance contract cannot be changed by any party. Moreover, vulnerability data, IoT device status data along with insurance policy data on blockchain could be used by proper party for risk score verification or insurance policy verification. Because of the public verification feature of the system, the insurer and the insured party have to follow the agreed contract without exception. In other words, insurer cannot pay lower coverage and insured party cannot obtain more coverage for any reasons which are not covered in the claim.

4.2.2 Privacy

The encryption of an IoT device's information with PEKS prevents the access of this sensitive information by other parties on the network. Since a blockchain provides authentication through a public key signature scheme, an adversary cannot fake any vulnerable IoT device to raise the rate of the insurance of the business entity. Additionally, the insurance company only is provided access to information that is necessary to calculate the risk score of the insured party's devices but has no access to additional sensitive information regarding the IoT devices as a result of the PEKS scheme.

4.2.3 Risk Rating Scheme as an incentive mechanism

As discussed previously, standard (cyber) insurance has a mostly predefined level of risk based on a small number of data points and observations such as surveys. With a static (or at least infrequently renewed) risk evaluation, insurance products are stuck having to charge premiums that reflect that standard risk in the entire market with only low levels of adjustment for the individual risk of the client. Since the insurance premium primarily reflects this analysis, insured parties have little incentive to improve their cyber security environment as they will benefit from the insurance regardless and will have the same premium cost without regard for security improvements[2]. In a Risk Rating Scheme such as the one described in this paper, we have the benefit of far more data points and being able to dynamically track both software vulnerability states as well as the vigilance with which client's attempt to resolve these vulnerabilities. By dynamically tracking and updating a client's insurance premium with these features, clients can see a direct economic benefit from routinely evaluating and resolving security problems in a timely manner. In this way, we create an incentive mechanism that provides an economic benefit to clients who actively resolve problems and improve the security state of their environment.

Based on the smart cyber scheme, expected profit/loss of insured company, insurers and society could be quantified with certain formula. The insured company will benefit from the decrease in the insurance premium when the risk score

[2] It is not to say that insurance companies cannot adjust premiums based on security improvements that are observed in a client's environment, but that there is usually no practical way to access this information in a reliable way that provides a faithful representation of the client's efforts or accomplishments

improves though it may require additional operating costs in order to maintain good security environment. In addition, it is likely that the expected loss caused by cyber incidents goes down as the probability of cyber attack decreases in better security state. In simple situation where contract is concluded at t=0 and the insurance premium (=f(Risk Score)) is adjusted only once at t=1 based on the change in risk score between t=0 and t=1, the calculation for the expected profit/loss for insured company is:

- Expected profit/loss = (Insurance premium at the time of contract) $\times \Delta f$(Risk Score)$-\Delta$(Operational costs)$+\Delta$(Probability of cyber attack)$\times$(Expected loss rate) $\times$ (Total exposure)

As for insurers, they will benefit from the decrease in the expected insurance loss incurred by cyber incidents while their revenue goes down when the risk score decreases.

- Expected profit/loss = (Total coverage) $\times$ Δ(Expected insurance loss) $-$ (Insurance premium at the time of contract) $\times$ Δf(Risk Score)

The impact on social welfare is difficult to estimate. But the increase in the risk score will entail the decrease in the number of vulnerable IoT devices, implying that the likelihood of catastrophic cyber attack and resulting social costs will go down. Thus, the insured company could be incentivized to improve the risk score when the positive effects, the decrease in premium and expected loss incurred by cyber attack, exceed the increase in operational costs. Likewise, insurers would have incentive to provide this type of products to mitigate cyber risk underwritten. Further study is needed to specify proper parameters and formula for the calculation of the premium so as to create sufficient level of incentives to each stakeholder.

4.3 Consideration on Regulation Issues

As discussed earlier, insurance products utilizing the smart cyber insurance scheme need to comply with regulatory requirement in order to get approval from insurance regulators. Given the traits of the scheme, we discuss issues should be especially considered before the commercialization in this section.

4.3.1 Validity and Accountability for the Calculation

Regulators might ask insurers to report details such as calculation model, risk score, premium and back data so as to assess the validity of dynamic pricing policy. In contrast to traditional insurance products which premium is fixed, the premium of smart cyber insurance products is periodically adjusted based on dynamic pricing model. Insurers and regulators would have to agree in advance on the degree and interval for the adjustment as regulators might deem that too volatile and frequent change in premium could harm interest of the policyholder[3].

Moreover, regulators might ask detailed explanation if the degree of discount by the risk score is much larger than the impact of other coefficients.

In addition, insurers are accountable for verifying that the scheme adequately capture the underwriting risk including accumulation risks and the risks are covered its capital. It should be noted that the risk and associated costs of cyber incidents such as data breaches could vary depending on multiple factors such as the IT development and regulation, indicating that insurers are required to address the change in situation (e.g. unexpected insurance loss incurred) by modifying the risk rating model or parameters.

On the other hand, it is desirable to achieve the mitigation of concentration risks of sensitive data that insurance companies have only encrypted data. Therefore, stakeholders of smart cyber insurance system should work together to strike a balance between privacy protection and insurer's accountability. For example, it is possible that other stakeholders such as IoT device managers provide regulators with necessary information for the supervisory purposes on behalf of insurance companies without sharing such data.

4.3.2 Future Work: Designing Optimal Supervisory Framework

While various regulators are trying to develop policy framework for cyber insurance market [4], there is still limited guideline or standard that fits for new types of cyber insurance like the smart cyber insurance scheme. For example, risk factors with regard to cyber insurance are not stipulated in law and regulation in many jurisdictions. It might make regulators face challenges in evaluating the appropriateness of the selected data, resulting in conservative judgement. Even though it is technically feasible to solve these issues, existing legal and supervisory framework may not allow such arrangement. Another example is security evaluation of smart contract used in smart cyber scheme, which is quite challenging for insurance regulators with limited knowledge and expertise about technology. In order to design and develop better regulatory environments, all stakeholders involved in the ecosystem should have a dialogue to develop common language and mutual understandings.

5 Conclusion

As the usage of Internet of Things devices proliferates in all aspects of business operations and personal electronics, the security risk they pose to their users and

[3] Smart cyber insurance scheme could be more difficult to understand than traditional one. From policyholder protection perspective, regulators might ask insurers to refrain from using complex pricing model especially when the products are sold to individuals.

[4] As an example, The EU-U.S. Insurance Dialogue Project began as an initiative by multiple organization including EIOPA, FIO and NAIC to enhance mutual understanding and cooperation between the European Union (EU) and the United States for the benefit of insurance consumers and business.

owners remains a concern. The usage of a smart cyber insurance scheme allows for the development of strong financial incentives to maintain safer IoT devices. The scheme should be applied to actual product design with considerations for regulatory goals and requirements. The inclusion of time-scaled premium calculations, the increased transparency between insureds and their insurers and the potential for the creation of dynamic insurance schemes acts to further the development of a more stable and secure Internet of Things ecosystem.

References

1. Information technology - security techniques - cybersecurity and iso and iec standards. Report ISO/IEC TR 27103:2018, ISO/IEC JTC1, 2018.
2. Walter Baer. Rewarding it security in the marketplace. *Contemporary Security Policy*, 24:190–208, 04 2003.
3. Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public key encryption with keyword search. volume 3027, pages 506–522, 04 2004.
4. Michèle Finck. Blockchain regulation and governance in europe. *Cambridge University Press*, 2018.
5. Corvus Insurance. Insurtech corvus launches smart cyber excess insurance with $10m limit. *Insurance Journal*, 2019.
6. European Insurance and Occupational Pensions Authority. Understanding cyber insurance - a structured dialogue with insurance companies. https://eiopa.europa.eu/Publications/Reports, 2018.
7. Petar Jevtic and Nicolas Lanchier. Smart contract insurance. https://blockchain.asu.edu/smart-contract-insurance/.
8. National Association of Insurance Commissioners. Report on the cybersecurity insurance and identity theft coverage supplement. https://content.naic.org, 2019.
9. International Association of Insurance Supervisors. Application paper on supervision of insurer cybersecurity. https://www.iaisweb.org/page/supervisory-material/application-papers, 2018.
10. EU-U.S. Insurance Dialogue Project. The cyber insurance market. https://eiopa.europa.eu/Publications, 2018.
11. Sasha Romanosky, Lillian Ablon, Andreas Kuehn, and Therese Jones. Content analysis of cyber insurance policies: How do carriers write policies and price cyber risk? *SSRN Electronic Journal*, 01 2017.
12. Daniel W Woods, Ioannis Agrafiotis, Jason Nurse, and Sadie Creese. Mapping the coverage of security controls in cyber insurance proposal forms. *Journal of Internet Services and Applications*, 8, 08 2017.
13. Daniel W Woods and Andrew Simpson. Policy measures and cyber insurance: a framework. *Journal of Cyber Policy*, pages 1–18, 08 2017.
14. William Yurcik and David Doss. Cyber insurance: A market solution to the internet security market failure. *In Proceedings of The 1st Workshop on the Economics of Information Security*, 2002.