A Novel Financial Instrument to Incentivize Investments in Information Security Controls and Mitigate Residual Risk

Pankaj Pandey
Gjovik University College, Norway
University of Antwerp, Belgium
Email: pankaj.pandey2@hig.no; pankaj.pandey@uantwerpen.be

Steven De Haes
Antwerp Management School, Belgium
University of Antwerp, Belgium
Email: steven.dehaes@uantwerpen.be

***Abstract*—Recent cyber-attacks on various organizations indicate that even the most sophisticated technical controls are vulnerable. Furthermore, due to the problem of misaligned incentives it is inevitable to achieve absolute protection with technical controls against the risks and its impact. Thus, there is a space for alternative risk management methods. However, there is a lack of an (effective) financial mechanism to incentivize coordinated efforts by stakeholders in addressing the problem of information asymmetry, negative externality, and free-riding in the information security ecosystem. Therefore, we propose a novel financial instrument called information security financial instrument to incentivize investments in collaborative and multistakeholder initiatives to develop and implement stronger defense systems. The mechanism can contribute to an improvement in information security environment in a time bound manner. We have used a case-study to demonstrate the application of the information security financial instrument. Furthermore, we have analyzed the information security financial instrument against a set of requirements and its usefulness over cyber-insurance in incentivizing investments in information security mechanisms to manage risks. In our analysis, we found that information security financial instruments can be a solution to address (at least to some extent) various economic problems in the information security domain.**

Keywords–Information Security; Security Economics; Risk Management; Financial Instrument.

I. INTRODUCTION

In today's technology-driven world, where organizations are heavily dependent upon information and communications technology, any attack on the technology infrastructure, and services offered over a computer network may lead to operational disruptions. The information and communication infrastructure (cyber ecosystem) face a wide variety of risks posed by a variety of threats such as distributed denial of services (DDoS) attacks, intrusion, eavesdropping, etc. These risks if materialized may have a huge negative impact on the organization including a negative impact on profits, brand value, and reputation. Furthermore, a successful cyber attack on the company may lead to negative impact on stock prices and overall corporate value [1]–[3]. Therefore, to reduce the likelihood and impact of the information (cyber) security risks, organizations have traditionally resorted to technical controls such as antivirus software, firewall, intrusion detection systems, intrusion prevention systems, and so on. However, cyber-attacks on various organizations such as JP Morgan [4], SONY [5], Target [6], and many more [4] indicate that even the most sophisticated technical controls are vulnerable.

When pursuing information security from an economic perspective, the failure of technical controls in providing 100% defense against the information security threats can be explained with the following reasons: (i) The problem of 'lemons market' [7], i.e., security product vendors do not have enough incentives to ship robust products in the market; (ii) The problem of misaligned incentives [8], i.e., information security stakeholders such as users (individual or organizations), security product vendors (e.g., McAfee, Symantec), cyber-insurance providers (e.g., Zurich Insurance) and regulatory bodies (e.g., financial markets regulator SEC in USA, Insurance regulator, regulatory bodies dealing with data protection and privacy, etc.) have misaligned incentives; (iii) The problem of 'tragedy of commons' [9], i.e., the issue of negative externalities and free riding in the network. In the light of the barriers mentioned above, it is inevitable to achieve near 100% protection against the risks and its impact, thus creating a space for *alternative risk management methods*.

Problem Statement: Lack of an (effective) financial mechanism to incentivize coordinated efforts of stakeholders in addressing the problem of information asymmetry, misaligned incentives, negative externality and free-riding in information (cyber) security ecosystem.

Motivation: Currently, cyber-insurance is only commercially available financial product that can be used to mitigate residual information security risks [10]. The proponents of cyber-insurance argue that it has the potential to align the incentives of security product vendors, users, and cyber-insurance providers, thereby creating a robust information security environment. However, there is a very little evidence to suggest that the cyber-insurance products can improve the network security by providing adequate incentives to organizations and individuals to invest aptly in information security controls [11][12].

Some researchers have mathematically proved that the cyber-insurance markets are inefficient [13][14]. These researchers have reported that though the cyber-insurance products satisfy all the other stakeholders but they fail to satisfy the regulatory bodies and sometimes the cyber-insurer provider itself. The regulatory bodies are unsatisfied due to the sub-optimal network robustness occurring due to under-investment in security controls by the network users. On the other hand, due to the interdependent and correlated nature of information security risks the uncertainty about the quantum of risk

 ISBN: 978-1-61208-427-5

exposure leads to the fear of systemic and huge losses for cyber-insurance providers. The notion of making no profits (or facing huge losses) in the future leads to dissatisfaction in cyber-insurance providers.

Thus, in absence of adequate market mechanisms for risk acceptance, the interest of entities who wish to transfer their risks and those who are willing to accept the risk by means of pooling and necessary expertise, are reduced [15].

Objective: To develop a financial instrument to address the problem of misaligned incentives and incentivize the stakeholders in making coordinated efforts in improving the information security ecosystem.

Contributions:

1) Developed a novel financial instrument called Information Security Financial Instrument (ISFI) to incentivize coordinated efforts of information security stakeholders (investors) in improving the information security ecosystem in a time bound manner.
2) Demonstrated the application of the financial instrument to improve the performance of a specific firewall.
3) Analyzed and explained the usefulness of the information security financial instruments in dealing with the problem of information asymmetry, negative externality and free riding in the information security domain. Furthermore, we analyzed the usefulness of the instrument as a risk management tool.
4) Contributed to the knowledge base of interdisciplinary research on information security economics.

The remainder of the paper is structured as follows: Section 2 presents an overview of the research method followed for the article. Section 3 presents an overview of the background work. Section 4 identifies the requirements for information security financial instruments. Section 5 describes the proposed information security financial instrument. Section 6 demonstrates the application of the proposed information security financial instrument. Section 7 presents an evaluation of the information security financial instruments. Section 8 concludes the article with conclusion and directions for future research.

II. Research Method

The research follows the Design Science Research Approach (DSRA). DSRA is useful when innovations and ideas are created for the development of technical capabilities and products that will be instrumental in effective and efficient process development for artifacts [16]. A process flow model for DSRA is shown in Figure 1.

A. Explicate Problem

The first step is to formulate the initial problem, justify its importance and investigate the underlying causes [16].

To explicate the problem we started with examining the literature on information security investment models, and currently available market methods and financial instruments for the management of information security risks. This enabled us in identifying the gaps in existing methods of (financial) risk management in information security domain. The identified problem is given as the problem statement in Section 1, and we have explained the background issues in Section 3.

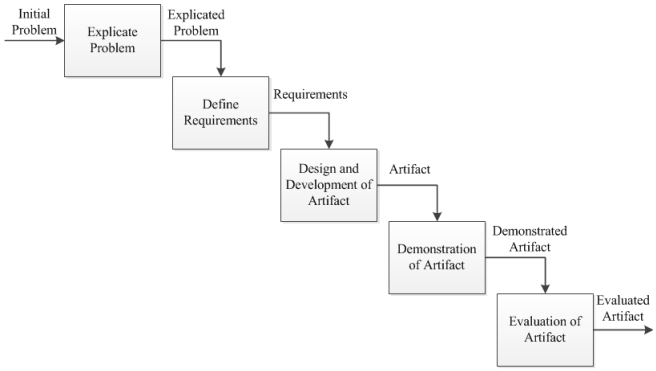

Figure 1. Process Flow Model for Design Science Research Approach [16].

B. Define Requirements

The second step is to identify and outline an artifact to address the explicated problem and to elicit requirements for the artifact [16]. A requirement is the property of the artifact that is desired by stakeholders in practice and is used for design and development of the artifact. A requirement can be functional, structural, or environmental in nature. The requirements for the artifact to address the problems identified in the previous step are given in Section 4.

C. Design and Development of the Artifact

The third step leads to the creation of an artifact that fulfills the requirements identified in the previous (second) step. This includes designing the functionality and structure of the artifact [16]. The functionality and structure of the artifact are explained in Section 5.

D. Demonstration of the Artifact

The fourth step proves the feasibility of the artifact by demonstrating its use in one case. Primarily, it consists of descriptive knowledge explaining the working of the artifact in one situation [16]. The demonstration shows that the artifact can, in fact, solve the problem (or some aspects of it) in the illustrative case. This demonstration can be considered as a weak form of evaluation. It indicates that if the artifact can address the problem in one situation; then it might be able to address the problem in other situations as well [16]. We have demonstrated the use of the artifact in Section 6.

E. Evaluation of the Artifact

The fifth step is to evaluate the artifact. This determines the extent to which the artifact can solve the explicated problem and its requirements [16]. An evaluation strategy can be an ex-ante or ex-post on the one hand and naturalistic or artificial on the other [16]. An ex-post evaluation implies that the artifact is evaluated without being fully developed or used. An ex-post evaluation implies that the artifact is evaluated after it has been implemented. A naturalistic evaluation implies that the artifact is evaluated in practice for which it is developed. An artificial evaluation implies that the artifact is evaluated in an artificial and contrived setting.

We have evaluated our artifact in Section 7 against the explicated problem and its requirements. We have used the 'informed argument' form of evaluation. Informed argument

 ISBN: 978-1-61208-427-5

form of evaluation is an ex-ante, artificial evaluation method, and it consists of arguments from the developers of the artifact [16]. In this case, researchers evaluate the artifact by reasoning and arguments for its usefulness in meeting the defined requirements and solving the explicated problem. Informed argument form of evaluation is often used to evaluate the artifacts that are highly innovative and are still immature [16].

III. Background Work

This section looks at the information security market from an economic perspective. In an efficient market for information security, buyers and sellers, both are expected to have sufficient information about the products. However, this is not currently the case. The information security goods are traded in markets with insufficient information similar to "The Market for Lemons" and "Market for Insurance". The following subsections explain the problems of information asymmetry, externality, and free-riding with the well-established economic theories.

A. The Market for Lemons

If the buyers lack information about the good and it then suggests that the sellers have sufficient information, then there is an asymmetry of information between the buyers and the sellers. This can be explained with the theory of "The Market for Lemons" proposed by George A. Akerlof [7]. Akerlof introduced "The Market for Lemons" with the question of why there is a "large price difference between new cars and those which have just left the showroom" [7]. He analyzed the rules of a market with information asymmetry between the buyer and the seller. He argued that a typical buyer of a used car cannot distinguish between the good cars and the bad cars (termed as "lemons"), as unlike the seller, the buyer does not know the true history of the used car. In such a scenario, the buyer is suspicious about the condition of the (good) car and is thus unwilling to pay more than the price of lemon (bad car). This type of market condition leads to under-supply of good condition used cars.

"The Market for Lemons" when mapped on to information security suggests that security product vendors do not have sufficient incentive to provide adequate security. It suggests that information security is a trust good and is not visible to the buyer. As a buyer cannot differentiate between the secure and insecure products, the product is traded at the price of insecure products (lemons). This leaves little incentive for the security product vendor to invest in the development of secure products. The security product vendor would rather prefer to have a less secure product and reach the market first to capture the market share or to invest in features that are more visible to the buyer.

B. Market for Insurance

Logically, it is unacceptable to suggest that only buyers lack the information and sellers have that information. Rothschild and Stiglitz examined the market of insurance as one "in which the characteristics of the commodities exchanged are not fully known to at least one of the parties" [17]. They claimed that "not only may a competitive equilibrium not exist, but when equilibria exist, they may have strange properties. In the insurance market, sales offers do not specify a price at which customers can buy all the insurance that they want, but instead consist of a price and a quantity – a particular amount of insurance that the individual can buy at that price. Furthermore, if individuals were willing or able to reveal their information, everybody could be made better off. By their very being, high-risk individuals cause an externality: the low-risk individuals are worse off than they would be in the absence of the high-risk individuals" [17]. This has an echo of "The Market for Lemons" but it is like a counter theory (mirror image) to Akerlof's work. Rothschild & Stiglitz assumed that "individuals know their accident probabilities, while companies do not" [17]. This is information asymmetry.

As discussed, the problem of information asymmetry has a negative effect on the insurance ecosystem, where it is difficult to distinguish between the high-risk and low-risk user types. This is commonly known as the problem of adverse selection. Similarly, users purchasing insurance policies when they know that they are highly likely to get affected, and they adversely affect the loss probabilities of the insurance providers. This is termed as the problem of moral hazard.

The theory of 'Market for Insurance' when mapped on to information security suggests that security product vendors know (at least to some extent) about the vulnerabilities in their products, however the users of the product are unaware about the vulnerabilities. Similarly, individuals and organizations purchasing cyber-insurance products have some information about the weaknesses in their defense system. However cyber-insurance providers lack a standard and evidence-based tool to check the strengths and weaknesses of the system. This information asymmetry leads to higher premiums, a large number of exclusions and the liability issue.

C. The Tragedy of Commons

The infrastructure of information and communication technology is largely interconnected and thus poses a challenge of collective security efforts by the participants. In economic terms, this can be explained with the theory of "Tragedy of Commons" proposed by Garrett Hardin [9]. According to the theory of the tragedy of commons, individuals acting rationally and independently in their self-interest with no consideration to long-term best interests of other members of the group would eventually lead to depletion of the common resources.

"The Tragedy of Common" when applied to information security domain explains the unwillingness of users to demand high security products. In a large distributed network, risks (and benefits) are spread over a set of nodes and are correlated. Thus, the information security is the property of the network and is not limited to its individual nodes. An investment in information security controls by one user to counter its risk exposure strengthens its security, and the node will strongly defend against the attacks. Thus, the benefit of defense gets propagated to other nodes in the network, and this is called 'positive externality'. Similarly, if the network is attacked, say by botnets, and one of the nodes gets corrupted then the risk of attack is propagated to other nodes leading to higher expected loss. In such a scenario, the cost (impact) of the attack is distributed between all the nodes. This is called 'negative externality'.

This suggests that the risks and benefits are all distributed between the nodes. This leads to a situation where individual nodes do not have a strong incentive to invest in information security unilaterally. They all tend to take a 'free-ride' on the

 ISBN: 978-1-61208-427-5

investments made by other nodes, thus depleting the common resource (security).

IV. Requirements for Information Security Financial Instruments

A report from World Economic Forum states that "No one organization can resolve the *(cyber-security)* issue by itself and a collaborative, multistakeholder approach must be taken; even competitors in a given industry must become partners in the effort to ensure a stable and trusted environment" [18]. Another report from World Economic Forum states that "Opportunities will emerge for new businesses in insurance or risk markets to help businesses mitigate the potential downside from cyber risks" [19].

As shown in Figure 2, Risk markets are one of the two ways to deal with systemic risk in information security domain [18]. Risk markets can provide a variety of financial instruments such as indemnification, insurance and structured risk-transfer solutions for an organization to address the information security risks [19].

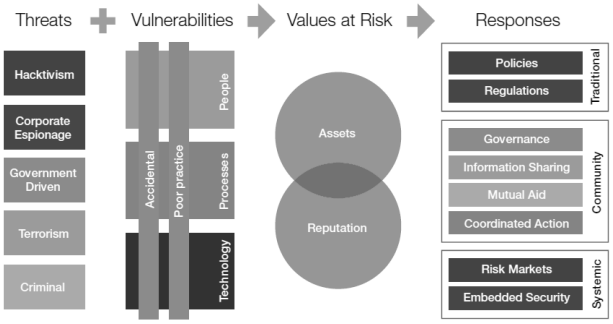

Figure 2. Cyber Risk Framework [18].

Therefore, keeping in view the problems identified in Section 3 of this article and the findings of World Economic Forum in [18][19], we have identified the following requirements for the Information Security Financial Instruments(ISFI):

Functional Requirements

- ISFI should incentivize coordinated efforts and investments in strengthening the security ecosystem.
- ISFI should tie the financial returns to the achievement of measurable or observable impact (performance or results), as specified in contract's specification.
- ISFI should fix accountability on the information security stakeholders, such as on project executors, or information security product vendors, to achieve the desired objectives.
- ISFI should clearly define the return structure.
- ISFI can be designed as an equity, debt or convertible instrument.

Usability Requirements

- Only verified traders/investors should be allowed to deal with ISFI.
- ISFI should be traded in a transparent environment.
- ISFI should be listed at (traded via) a regulated platform.
- ISFI should allow anonymous trading/investing.
- ISFI should be traded in a manipulation resistant environment.
- ISFI should be traded at low transaction cost.
- ISFI should be traded in a liquid environment.

V. Information Security Financial Instrument

This section presents a novel financial instrument, called Information Security Financial Instrument (ISFI) to incentivize investments in collaborative and multistakeholder initiatives to develop and implement stronger defense systems. The returns on ISFI are linked to the achievement of certain security objectives and mitigation of underlying risks. An application scenario for ISFI is shown in Figure 3.

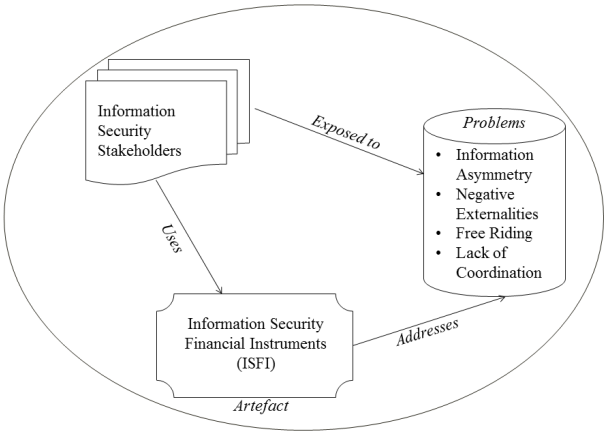

Figure 3. An Application Scenario for ISFI.

The ISFI can be implemented in at least following two forms:

- **Results based Information Security Financial Instruments:** This type of instruments provides a mechanism and strategies designed to tie purposefully the investments in information security controls and risk mitigation methods and thus incentivize the efficient allocation of resources provided by security stakeholders. Properly designed and well-implemented results based information security financial instruments may result in improvement in quality and timely delivery of (more) secure products, lower risk exposure, a shift towards a result oriented rather than a ship next day approach, and an improved security ecosystem. However, these benefits come at the expense of some opportunity costs, the need to monitor and test the performance, and exposure to the risk of incorrect incentive system.
- **Information Security Performance Instruments:** Information security performance instruments, if designed properly, can be helpful in achieving the long-term improvement in the information security ecosystem, increasing efficiency and creating a favorable environment to attract investment capital. Information security performance instruments can be designed to meet security goals for critical public infrastructure

 ISBN: 978-1-61208-427-5

such as power grids, in the oil and gas sector, financial sector and others, and include time-bound performance goals against which the performance of the service operator is measured. ISFI can be useful in sourcing funds for the projects where traditional funding sources are not (or less) useful.

The process of designing an information security financial instrument is shown in Figure 4.

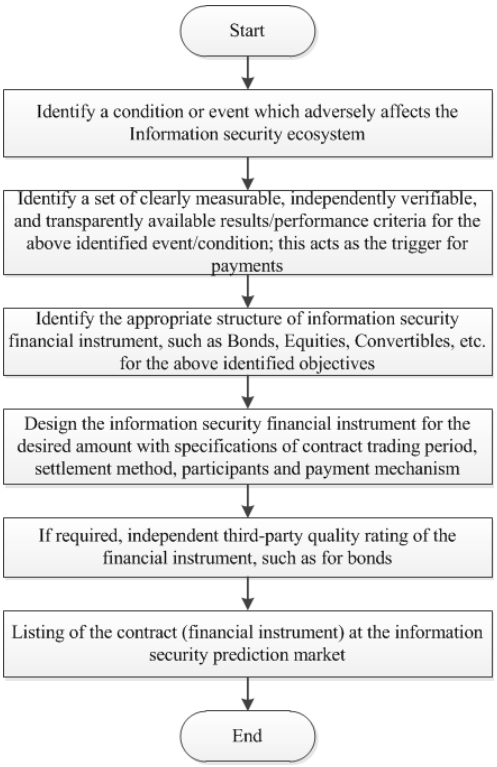

Figure 4. Process of Designing and Trading an ISFI.

The six processes shown in Figure 4 are explained in the following subsections.

A. Identification of Security Objectives

The design of useful information security financial instruments to incentivize investments in improving cyber-defense systems and risk mitigation depends upon the identification of useful 'objectives'. The incentive system depends upon the achievement of desired and predefined underlying security objectives to which returns are linked.

The underlying objectives of an information security financial instrument can be structured in at least the following five ways:

- *Reductions*: For example, reduction in number of vulnerabilities in a piece of software.
- *Improvements*: For example, improvement in the cyber-intelligence tool used by a law enforcement agency.
- *Increasing*: For example, increase in the detection of new viruses in the cyber space.
- *Decreasing*: For example, decrease in the false acceptance rate of a biometric authentication system.
- *Compliance Goals*: For example, meeting the industry compliance and regulations, such as HIPAA, SOX, etc., and thus avoiding any fine for violation of the norms.

Table 1 presents a set of entities (stakeholders) that can play a vital role in identification of the underlying objectives for information security financial instruments.

TABLE I. TYPICAL STAKEHOLDERS OF ISFI.

Issuer	Issuer entity can be a government body, regulatory body or a financial institution interested in achieving an information security objective. Also, an industry body charged with the responsibility of achieving specific goals or a beneficiary of achievement of objectives can be an issuer. Cyber-Insurance providers, Reinsurance providers, security product vendors, etc., can be instrumental in identifying the information security objectives for which financial instruments are to be issued.
Investors	Investors are interested in allocating capital and resources to fund large scale information security projects (critical infrastructure like power grids, implementation of privacy policy at a country/industry/EU level, etc.), earn profits tied to the achievement of objectives, and hedge the risks associated with the underlying objectives. Insurance providers, reinsurance providers, project executors, users, etc., can be investors.
Executors	They are the entities with the responsibility of achieving the objectives as specified in the contract (financial instrument) description. Depending upon the underlying objectives, executors can be software product vendors, vendor's competitors, security researchers, etc.
Clearing House	Clearing house acts as an inter-mediator between the issuer, investors and executors. Clearing house manages the credit risk, trader/investor verification, acts as an absolute authority on settlement of contracts, and an independent third party for the verification of claims.

Furthermore, it is not necessary to have clear demarcation of roles between the above entities and multiple functions can be performed by a single or a combination of above entities.

B. Identification of Payment Trigger Criteria

The payment trigger criteria should be clearly defined, be measurable or impact observable, transparent, and verifiable by an independent third party. Further, the contract specification on the trigger criteria should avoid any present and foreseeable conflict of interests between the issuing entity and other administrative stakeholders.

The ISFIs can be structured with various types of measurable and observable impact criteria, such as 'reduction' (e.g., 2%, 5%, etc.) in number of vulnerabilities discovered in a piece of software (thereby making the software more secure), an 'increase' (e.g., 3%, 7%, etc.) in accuracy of a new biometric based authentication system, and so on.

Table 2 presents a set of payment trigger criteria for ISFIs (equities, bonds, and convertibles).

C. Types of Financial Instruments

The ISFI can be designed as 'debt', 'equity', or 'convertible' instruments.

- *Debt Instrument:* A debt instrument is a contract between a lender and a borrower under which borrower borrows money in exchange of payments of the principal amount and fixed interests over a defined period. One such instrument is a 'bond'.
  The issuer i.e., the indebted entity issues a bond specifying the coupon i.e., interest rate that will be paid with the principal amount on the maturity date. The

 ISBN: 978-1-61208-427-5

TABLE II. PAYMENT TRIGGER CRITERIA FOR ISFI.

Trigger Criteria	Examples
Performance Index	Such as ISE Cyber Security ETF (HACK) [20], UK Cyber Vulnerability Index [21], Global Cybersecurity Index (GCI) [22], Index of Cyber Security [23]
Results Indicators	Such as Technological Indicators (improvement in performance of antivirus software,firewall, etc.), Process and Procedural Indicators (compliance with data management & privacy policies, such as deletion of user data after certain period, etc.), so on.
Customized Indicators	Such as a combination of performance index and result indicators, Qualitative analysis of security strength, penetration of antivirus, firewall and other security defense systems, so on.

two key features that determine the interest rate on the bond are duration and credit quality. An independent third party can be involved to certify the credit quality of the bond.

- *Equity Instrument:* Equity instruments are tradable assets i.e., tradable capital packages with unique structures and characteristics. Equity instruments are different from debt instruments in a way that they provide some control and ownership of the business. A commonly known equity instruments is stock.
- *Convertible Instrument:* Financial instruments that can be converted to common stocks are known as convertibles, such as bonds and preferred shares. For example, holders of convertible bonds are allowed to convert their position to equities at an agreed price.
  Convertible financial instruments are attractive to investors looking for higher returns than bonds and equities. For example, convertible bonds will have lower coupon rate than traditional bonds. However, the option of converting the bond to common stocks provides an added value to the holder.

Table 3 presents three types of ISFIs and corresponding trigger criteria for payments.

TABLE III. TYPES OF ISFI AND PAYMENT TRIGGER CRITERIA.

ISFI Type	Payment Trigger Criteria
Information Security Equity	Result Indicators
Information Security Bonds	Performance Indices
Information Security Convertibles	Pre-specified Indicators

D. Contract Specifications

Next step in the process of creation and trading of ISFIs is the specification of contracts. We have identified a set of specifications which needs to be considered when creating an ISFI. Table 4 presents a template with the specifications identified for the information security contracts.

E. Return Structure

The returns on ISFIs can be structured in a variety of ways depending on the objectives of the issuing entity. The triggers for returns are linked to the achieving the specific objectives as specified in the contract description. Table 5 presents a set of return structures for ISFIs.

The ISFIs can be designed with other types of return structures, or a combination of return structures can be used.

TABLE IV. TEMPLATE FOR SPECIFICATIONS OF ISFI.

Issuer	
Objective of the Funding	
Benchmark Measurement Criteria	
Total Funding Required	Amount : Currency :
Project Start Date	
Project End Date	
Information Security Financial Instrument Type	
Transferable Instrument	
Decision Criteria	
Initial Benchmark Value	
Minimum Investment Required	Amount : Currency :
Eligible Investors	
Independent Third Party Quality Rating Required	Yes/No
Independent Third Party Verification Required	Yes/No
Management Fee	
Know Your Trader/Investor Required	Yes/No
Return Structure	
Pay-Off Horizon	
Bonus Payment	Yes/No
Trigger for Bonus Payment	If applicable

TABLE V. RETURN STRUCTURE FOR ISFI.

Fixed Return Structure	The returns i.e., bond yields or stock dividends are fixed and based on achievement of pre-determined objective. For instance, improvement in performance of 'XYZ' firewall in defending against 'UVW' types of attacks by 10% in 01 year will provide a return of 3%
Increasing Return Structure	In this case, returns are proportionately linked to increase in performance or quality or impact outcomes. For instance, for every 1% improvement in performance of 'XYZ' firewall in defending against 'UVW' type attack will provide 0.1% return
Tiered Return Structure	In this structure, returns depend upon the level of outcomes, i.e., the return structure is tiered (increase or decrease). For instance, a 5% improvement in performance of 'XYZ' firewall will yield 3% return, and an improvement of 10% will yield 7%, and so on.
Decreasing Return Structure	In this structure the return decreases with decrease in performance outcomes. This leads to reduction in interest disbursements and thus, creates a tangible reward for the issuing entity.

For instance, a fixed return structure can be used up to a certain level and then a tiered return structure is used, etc.

The structure of ISFIs will depend upon the specific information security objectives of issuing entity. For instance, for improvement in performance of a particular cyber-intelligence tool which is used by government organizations and has been developed by or in collaboration with a private organization, then a tiered return structure can be used for the ISFI. In this case, the instrument will have a base return and a bonus return will be awarded if the performance of the said cyber-intelligence tool is assessed to be above the threshold as specified in the contract (financial instrument) specifications. Table 6 presents a set of ISFIs, respective return structures and trigger criteria.

TABLE VI. ISFI, RETURN STRUCTURE, AND TRIGGER CRITERIA.

ISFI Type	Return Structure	Trigger Criteria
Bonds	Fixed Return	Performance Index
Equity	Increasing Return	Result Indicators
Convertibles	Decreasing Return	Customized Indicators
Convertibles	Tiered Return	Customized Indicators

 ISBN: 978-1-61208-427-5

F. Listing of Contracts

Once the ISFIs are created they can then be traded over-the-counter (OTC) or they can be listed at the information security prediction market to allow trading of the contracts. Information security prediction market is the preferred platform, as it is expected to facilitate information elicitation, trading transparency, lower transaction cost, liquidity, efficiency and manipulation resistance.

VI. Example Application

In this section, we demonstrate the application of ISFI in improving the performance of firewalls developed by Europe-based organizations against a particular 'UVW' type of attacks. As Firewalls are the first line of defense against information security attacks, an improvement in performance of firewalls is highly important in addressing the 'public goods' nature of information security and addressing the problem of negative externality and free riding. An application scenario of information security bonds in strengthening the security ecosystem is shown in Figure 5.

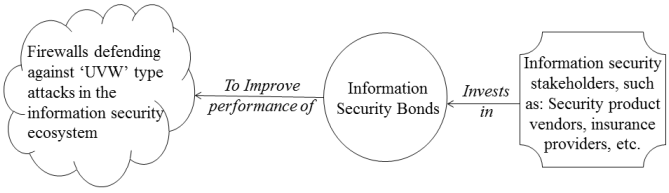

Figure 5. Application of ISFI in Strengthening Information Security Ecosystem.

An information security bond issued by the association of information security product vendors in Europe, to improve the performance of firewalls developed by Europe based organizations to defend against the 'UVW' type of attacks is shown in Table 7.

If an investor invests USD 100,000 in the information security bond shown in Table 7, then the investor will earn returns based on the average performance of firewalls against the 'UVW' type attacks as shown in Table 8.

TABLE VIII. RETURNS ON INVESTMENT OF USD 100,000 FROM INFORMATION SECURITY BONDS.

Result	Performance Score on 31/Dec/2017	Return	Returns to Investors
Performance unchanged	10	10%	$10,000
Performance improves by 10%	11	20%	$20,000
Performance improves by 20%	12	25%	$25,000
Performance improves by 30%	13	30%	$30,000

As shown in Table 7 and Table 8, information security stakeholders can coordinate their efforts in strengthening the information security ecosystem and can reap significant profits from the financial instruments.

VII. An Evaluation of ISFI

The artifact evaluation consists of three sub-activities [16]. The first activity 'analyze context', analyzes and describes the context of evaluation. The second, 'select goals and strategy', is not only about deciding the goals and strategy for the evaluation but also about selection of research strategy and methods. The third sub-activity, designs the evaluation study and then executes the same.

Figure 6 shows the artifact (ISFI) evaluation process.

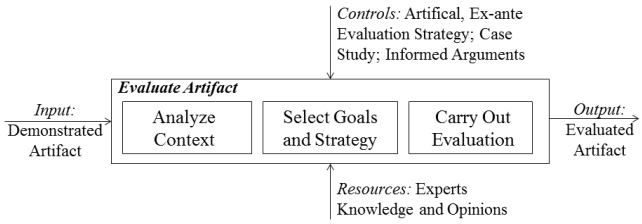

Figure 6. ISFI Evaluation Process (adapted from [16]).

- *Input:* describes the knowledge or object which is the input to evaluation activity.
- *Output:* describes the knowledge or object which is the outcome of the evaluation activity.
- *Controls:* describes the knowledge that is used for evaluation activity, including evaluation strategies.
- *Resources:* describes the knowledge which is used as the basis for the evaluation exercise, i.e., the knowledge base.

A. Analyze Context

The first sub-activity is 'Analyze Context', and it primarily identifies the constraints in the evaluation environment [16]. The main constraint in the evaluation of ISFI are the technological, financial, legal and time constraints.

B. Select Goals and Strategy

The second sub-activity 'Select Goals and Strategy' is based on the evaluation context. The goals selected are to evaluate the ISFI against the identified requirements, and its usefulness in addressing the previously identified problems, using formative evaluation. One of the six evaluation types stated in [24] is to 'Comparison'. It implies that the artifact is not evaluated in isolation indeed it is studied in comparison to other artifacts meant for the same or similar purpose. Therefore, where necessary, we have compared our artifact with cyber-insurance products. The evaluation strategy selected is artificial, and ex-ante. The ISFI is evaluated using an 'informed argument' strategy. The formative evaluation is chosen because the results of the evaluation may lead to several iterations before the design of ISFI is finalized.

C. Carry Out Evaluation

The evaluation consists of two parts. First, to evaluate the artifact against the ISFI requirements. Second, to evaluate the usefulness of ISFI.

1) Evaluation against ISFI Requirements: The following evaluation is only for the functional requirements of ISFI. As the usability requirements (and their achievements) are dependent upon the mechanism facilitating the trading/investment in the instrument, thus the usability requirements should be evaluated with respect to the platform. Therefore, the evaluation of usability requirements is beyond the scope of this evaluation.

TABLE VII. AN EXAMPLE APPLICATION OF INFORMATION SECURITY FINANCIAL INSTRUMENTS.

Issuer	Information Security Product Vendors Association
Objective of the Funding	To improve the performance of firewalls developed by Europe based companies to defend against UVW type attacks in two years
Benchmark Measurement Criteria	Firewall performance index against UVW type attacks
Total Funding Required	Amount : 1,000,000; Currency : USD
Project Start Date	01-Jan-2016
Project End Date	31-Dec-2017
Information Security Financial Instrument Type	Information Security Bond
Transferable Instrument	Yes, only to verified traders/investors registered with the clearing house/information security prediction market
Decision Criteria	The average performance of firewalls developed by European companies against the UVW type attacks must improve by at least 10% before the project end date.
Initial Benchmark Value	Let us assume that there are three firewalls developed by European companies and providing defense against UVW type attacks and each has a global market coverage of at least 30% *Firewall 1 :* Average Performance Index between 01-Jan-2015 to 31-Dec-2015 is 10 *Firewall 2 :* Average Performance Index between 01-Jan-2015 to 31-Dec-2015 is 8 *Firewall 3 :* Average Performance Index between 01-Jan-2015 to 31-Dec-2015 is 12 Average Performance Index for the three firewalls between 01-Jan-2015 to 31-Dec-2015 is 10
Minimum Investment Required	Amount : 10,000; Currency : USD
Eligible Investors	Information Security Product Vendors, Cyber-Insurance Providers, Reinsurance Providers, Information Security Researchers, Security Industry Consortium, Investment Managers, Product Users
Independent Third Party Quality Rating Required	Yes, for credit rating of issuer
Independent Third Party Verification Required	Yes, for the performance evaluation of the firewall
Management Fee	2%
Know Your Trader/Investor Required	Yes, verification of personal and minimal financial background of participants.
Return Structure	Mixed (Tiered and Incremental) Base Return: 10% irrespective of firewall performance index after two years. The incremental returns are linked to the actual performance outcome of firewalls developed by European companies as below: *(i) Base Yield = 10%*; *(ii) 10% above the reference = 20%* *(iii) 20% above the reference = 25%*; *(iv) 30% above the reference = 30%* For performance between the above tiers, returns are calculated on pro-rata basis.
Pay-Off Horizon	07 days from the project end date
Bonus Payment	Yes
Trigger for Bonus Payment	As specified in return structure section

- *Coordinated Efforts and Investments:* In the absence of efficient and effective cyber-insurance markets, incentives to engage in prevention and insurance are reduced. In the absence of an effective cyber-reinsurance market, the government is expected to become the financier of huge systemic losses [25]. Alternatively, governments can encourage the information security stakeholders to engage in risk financing through ISFI that, in turn may cover the risk exposures. ISFIs can provide a project based approach to manage systemic risk through mitigation or risk transfer, will reduce specific 'threat/vulnerability' exposure and may lead to better risk management practice, thus strengthening the information security ecosystem.
  ISFIs can be used as a mechanism to combine risk exposures spread over several information security defense products. This can be achieved by pooling the systemic risk exposure across the product types to provide a natural first line of defense by engaging the stakeholders in coordinating the efforts to strengthen the information security ecosystem. It may also provide a scale economics to finance risk arrangements in international information security markets.
  As demonstrated in Section 6, an ISFI (bond) is used to engage various information security stakeholders particularly the companies developing firewalls in Europe and providing a defense against 'UVW' type attacks. Through the information security bonds, these firewall developers can invest in coordinated efforts to improve the performance of their firewalls to defend against the 'UVW' type attacks. After the end of the project, the project (performance) data can be used to market their firewalls as a (more) effective product, thereby better positioned against the firewall developers from other regions.
- *Tied Returns:* The combination of higher event frequency and extended exposure increase the potential damages. Despite the growing information security risk exposure, cyber-insurance markets are not mature and effective enough to counter the risks. Therefore, most of the organizations (and individual users) are exposed to information security risks and do not have (adequate) financial coverage. Given the fact, a 'proactive' use of alternative risk management mechanism may be worth considering.
  ISFI can provide a 'proactive' mechanism for information security risk management. To achieve this, returns on ISFI are tied to the achievements of pre-specified performance or results expectations. These payment triggers are clearly defined, objectively measurable and independently verifiable.
  As demonstrated in Section 6, ISFI (bonds) are issued with an objective of improving the performance of firewalls developed by Europe-based companies, and the returns are tied to the 'firewall performance index'.
- *Accountability:* Researchers, industry practitioners and the legal fraternity have been arguing for a very long time over the issue of software 'bug/vulnerability' liability [26]–[29]. However, the discussion on the topic remains inconclusive. ISFI aims to target this issue by fixing the accountability on the stakeholders (such as on a product vendor) to fix the bug or to reduce the number of bugs in a piece of software in lieu of returns tied to the achievement of the same.

 ISBN: 978-1-61208-427-5

As demonstrated in Section 6, the 'information security product vendors association' is the issuer and owns the accountability to achieve the desired performance of firewalls against the specified attacks. A failure to achieve the desired performance is likely to result into losing the competition to others, facing the opportunity cost, and so on.

- *Return Structure:* ISFI provides a variety of return structure depending on the objective of the issuer and other security stakeholders. The payment triggers are linked to the achievement of pre-specified performance or observable results.
  As demonstrated in Section 6, the information security bond provides a mixed return structure. It incentivizes achievement of as high as the possible performance of the firewall, so as to earn maximum possible returns based on the incremental tier structure.
- *Designed as Equity, Debt or Convertible Instrument:* ISFI are tailor made products to address the specific (underlying) problems or objectives. Therefore, to cater to the variety of objectives, events, and needs of security stakeholders, ISFI have the flexibility to be designed as equity, debt, and convertibles.
  As demonstrated in Section 6, ISFI is a bond type instruments designed to source funds to improve the performance of firewalls. Similarly, equity and convertible types of instruments can be drawn to meet specific functional requirements.

2) Evaluation against ISFI Usefulness: The evaluation of ISFI against its usefulness in dealing with the problem of information asymmetry, negative externality, and free riding is as follows:

- *The Market for Lemons:* ISFI targets the problem of information asymmetry where sellers have no (or minimal) incentive in producing robust products. ISFI can be used as a method to prove the performance of the target products.
  For instance, as demonstrated in Section 6, the firewall vendors can use the performance data of the information security bond to prove that their firewalls are better than the other (lemons) firewalls providing defense against the UVW type attacks. This works as a product rating or quality assurance for the buyer. In such a scenario, firewall vendor with proven performance of the firewall may charge a higher price than its competitors (i.e., lemons).
- *The Market for Insurance:* ISFI can be used to address the problem of 'market for insurance'. In such a scenario, customers willing to purchase cyber-insurance policies can prove the resilience of their information security defense system by using the software, hardware and practices & policies, which have achieved a certain level of performance as exhibited through ISFI. This will create a level of confidence in the cyber-insurance provider, and the insurance buyer can negotiate for a lower premium or inclusion of certain other risk coverage.
  For instance, as demonstrated in Section 6, a user using one of the firewall which achieved the desired performance as per the information security bond can claim a better protection against UVW attacks compared to those who are using other firewalls and thus negotiate for a lower premium.
- *The Tragedy of Commons:* ISFI targets the problem of negative externality and free riding by incentivizing the coordinated efforts of various stakeholders. ISFI encourages investments in robust security products, and visibility of quality and performance of these products will lead to natural robustness in the ecosystem.
  For instance, as demonstrated in Section 6, if the information security bonds lead to achievement of desired performance of the firewalls then the government can bring in mechanisms like tax credit [30] to encourage usage of proven security products and wide acceptance of these products will help in eliminating the issue of negative externality and free riding from the information security ecosystem.

VIII. Conclusion and Future Work

In this paper, we have shown a need for an alternative risk management method. We have identified a set of requirements for Information Security Financial Instruments (ISFI) which can be used as an alternative risk management mechanism to incentivize coordinated efforts by security stakeholders in strengthening the information security ecosystem. We have designed the ISFI and demonstrated its application with an imaginary case of improving firewall performance. Then, we analyzed the ISFI against the set of functional requirements and its usefulness in addressing various economic problems prevalent in information security domain. In our analysis, we found that the ISFI meets all the functional requirements for the instrument. Also, on the issue of addressing the problems of information asymmetry, negative externality and free riding, ISFI can be highly useful. However, as our analysis is based on 'informed argument' evaluation method, the evaluation faces a high risk of false positives.

There are three limitations in the paper: (i) ISFI is demonstrated with a 'bond' type instrument only. Application of equity and convertible type instruments are not presented and left to the future work. (ii) Our evaluation of ISFI is only for the functional requirements; however usability requirements may have a significant impact on success or failure of the instrument, and this is left for future work. (iii) We have demonstrated and evaluated the ISFI based on an imaginary case; however there could be several constraints when implementing the instrument in a naturalistic setting.

References

[1] L. A. Gordon, M. P. Loeb, and L. Zhou, "The impact of information security breaches: Has there been a downward shift in costs?" Journal of Computer Security, vol. 19, no. 1, Jan. 2011, pp. 33–56.

[2] B. Cashell, W. D. Jackson, M. Jickling, and B. Webel, "The economic impact of cyber-attacks," Government and Finance Division, Congressional Research Service,, CRS Report for Congress Order Code RL3233, April 2004.

[3] A. Smith. Share prices are rarely hit hard by cyber attacks. Financial Times. http://www.ft.com/intl/cms/s/0/348d7f1a-417e-11e3-9073-00144feabdc0.html. [retrieved: Apr, 2015]

[4] D. Y. Emily Glazer. J.p. morgan says about 76 million households affected by cyber breach. Wall Street Journal. [Online]. Available: http://www.wsj.com/articles/j-p-morgan-says-about-76-million-households-affected-by-cyber-breach-1412283372 [retrieved: Apr, 2015]

 ISBN: 978-1-61208-427-5

[5] J. Tom Huddleston. What you need to know after sony's hacker attack. Fortune. [Online]. Available: http://fortune.com/2014/12/03/need-to-know-cyber-attacks/ [retrieved: Apr, 2015]

[6] H. Kuchler and A. Raval. Target data theft sounds wake-up call for retailers. Financial Times. http://www.ft.com/intl/cms/s/0/7d5f28bc-7d81-11e3-81dd-00144feabdc0.html. [retrieved: Apr, 2015]

[7] G. A. Akerlof, "The market for 'lemons': Quality uncertainty and the market mechanism," Quarterly Journal of Economics (The MIT Press), vol. 84(3), 1970, pp. 488–500.

[8] R. Anderson, T. Moore, S. Nagaraja, and A. Ozment, Algorithmic Game Theory, 2007, ch. Incentives and Information Security, pp. 633–649.

[9] G. Hardin, "The tragedy of the commons," Science, vol. 162, 1968, pp. 1243–1248.

[10] E. R. McNicholas. Cybersecurity insurance to mitigate cyber-risks and sec disclosure obligations. The Bureau of National Affairs, Inc. http://www.bna.com/cybersecurity-insurance-to-mitigate-cyber-risks-and-sec-disclosure-obligations/. [retrieved: Apr, 2015]

[11] Zurich American Insurance Company vs Sony Corporation of America, no. No. 651982/2011. NewYork Supreme Court, Jul 2011.

[12] R. King. Cyber insurance capacity is very small: Aig ceo. CIO Journal. Wall Street Journal. [Online]. Available: http://blogs.wsj.com/cio/2015/04/02/cyber-insurance-capacity-is-very-small-aig-ceo/ [retrieved: Apr, 2015]

[13] M. Lelarge and J. Bolot, "Economic incentives to increase security in the internet: The case for insurance," in INFOCOM 2009, IEEE. IEEE, 2009, pp. 1494–1502.

[14] Z. Yang and J. C. Lui, "Security adoption and influence of cyber-insurance markets in heterogeneous networks," Performance Evaluation, vol. 74, no. 0, 2014, pp. 1 – 17.

[15] K. J. Arrow, "Uncertainty and the welfare economics of medical care," The American Economic Review, vol. 53, no. 5, 1963, pp. 941–973.

[16] P. Johannesson and E. Perjons, An Introduction to Design Science, 1st ed. Springer International Publishing, 2014, iSBN: 978-3-319-10631-1.

[17] M. Rothschild and J. Stiglitz, "Equilibrium in competitive insurance markets: an essay on the economics of imperfect information," Quarterly Journal of Economics, vol. 90, 1976, p. 629.

[18] WEF and Partners, "Partnering for cyber resilience: Risk and responsibility in a hyperconnected world - principles and guidelines," World Economic Forum, Tech. Rep. Ref. 270912, March 2012.

[19] WEF and Partner, "Risk and responsibility in a hyperconnected world," World Economic Forum in collaboration with McKinsey & Company, Tech. Rep., Jan 2014.

[20] "Purefunds ise cyber security etf," Pure Funds, Tech. Rep., 2014. [Online]. Available: http://pureetfs.com/etfs/hack.html

[21] "Uk cyber vulnerability index 2013," KPMG Consulting, Business and industry issue, May 2014.

[22] "Global cybersecurity index," International Telecommunication Union and ABI Research, Tech. Rep., 2014.

[23] Index of cyber security. [Online]. Available: http://www.cybersecurityindex.org/ [retrieved: Apr, 2015]

[24] J. Venable, J. Pries-Heje, and R. Baskerville, "A comprehensive framework for evaluation in design science research," in Design Science Research in Information Systems. Advances in Theory and Practice. Springer, 2012, pp. 423–438.

[25] A. Gray. Government resists calls to fund backstop for cyber disaster losses. Financial Times. [Online]. Available: http://www.ft.com/cms/s/0/7f9d8326-d096-11e4-a840-00144feab7de.html [retrieved: Apr, 2015]

[26] R. Clarke, "Who is liable for software errors? proposed new product liability law in australia," Computer Law & Security Review, vol. 5, no. 1, 1989, pp. 28 – 32.

[27] J. Armour and W. S. Humphrey, "Software product liability," School of Law, University of Pittsburgh and SEI, Carnegie Mellon University, USA, Tech. Rep. CMU/SEI-93-TR-13, ESC-TR-93-190, Aug 1993.

[28] J. Goodchild. Security experts: Developers responsible for programming problems. [Online]. Available: http://www.csoonline.com/article/2124824/malware-cybercrime/security-experts--developers-responsible-for-programming-problems.html [retrieved: Apr, 2015]

[29] M. Masnick. U.k. court says software company can be liable for buggy software. [Online]. Available: https://www.techdirt.com/blog/innovation/articles/20100513/0053499408.shtml [retrieved: Apr, 2015]

[30] 113th Congress (2013-2014), Ed., Cyber Information Sharing Tax Credit Act, no. S.2717, Senate of the United States. Senate - Finance, July 2014. [Online]. Available: https://www.congress.gov/bill/113th-congress/senate-bill/2717/text

 ISBN: 978-1-61208-427-5