RiSKi: A Framework for Modeling Cyber Threats to Estimate Risk for Data Breach Insurance

Angeliki Panou
Department of Digital Systems,
University of Piraeus
P.O. Box 18534
Greece
apanou@unipi.gr

Christoforos Ntantogian
Department of Digital Systems,
University of Piraeus
P.O. Box 18534
Greece
dadoyan@unipi.gr

Christos Xenakis
Department of Digital Systems,
University of Piraeus
P.O. Box 18534
Greece
xenakis@unipi.gr

ABSTRACT

Historically, the financial benefits of cyber security investments have not been calculated with the same financial discipline used to evaluate other material investments. This was mainly due to a lack of readily available data on cyber incidents impacts and systematic methodology to support the efficacy of cyber investments. In this paper we propose an innovative, cyber investment management framework named RiSKi that incorporates detection and continuous monitoring of insiders societal behavior, to the extent permitted by the law, to proactively address implied anomalies and threats and their potential business impact and risks. Moreover, it provides access to published security incidents data to enable businesses to advance their understanding of cybersecurity and awareness of the threats and consequences related to cyber breaches, and, eventually, enable faster recovery from an event. RiSKI armed with the above information, employs a methodology, and develops a supporting scenario-based cyber investment tool, for quantifying the benefits of cybersecurity investments against the many ways that potential cyber risks can affect the operation of a business.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy** → Economics of security and privacy

KEYWORDS

Cyber insurance, Optimal Investment, Risk analysis, serious games.

PCI 2017, September 28–30, 2017, Larissa, Greece

ACM ISBN 978-1-4503-5355-7/17/09…$15.00
https://doi.org/10.1145/3139367.3139426

1 INTRODUCTION

Cyber threat remains one of the most significant - and growing - risks facing EU business, (i.e., in 2016 more than 1.1 billion identities were stolen in data breaches, almost double the number stolen in 2015) [1]. On the other hand, the new EU data protection framework, namely, the General Data Protection Regulation (GDPR) [2], is a game-changer for companies that process data, introducing changes in three key points: a) accountability, where companies are responsible for building data protection and privacy into their organizational design; b) notification, which obliges companies to notify the authorities of all breaches that put individuals at risk; and c) properly informed consent for the use of data. Since GDPR will come into force in mid-2018, the involved stakeholders need to start making changes now, if they want to be ready to meet their new obligations and avoid potentially crippling new fines for getting things wrong. Because of the high fines, cybercrime can no longer be considered as an acceptable 'running cost' of business. Therefore organizations are interested in minimizing their risk exposure by proceeding to optimal investments in cyber security solutions and procedures, while transferring the residual risk to cyber insurance.

However, both optimal security investments and insurance premiums cannot be accurately calculated because of the existence of the following limitations:

1. The multidisciplinarity of the problem of cyber threats, which except for the technological dimension, it has to be carefully studied, analysed and understood also from societal, organization, regulatory and economic points of view as well as their interdependencies.
2. The rapidly changing cyber landscape, which implies that historical data often do not reflect the current threat environment. Hence, it is not possible for decision-makers and insurers to use traditional approaches to model loss distributions.
3. The lack of verified risk management methodologies that follow an approach of commonly agreed metrics and provide quantitative results, considering both tangible and intangible assets.
4. The absence of effective applied econometric models that guide and estimate the optimal investment in security solutions and controls, (i.e., at both technical

and organizational level), in order to mitigate or eliminated the estimated risks.

5. There is limited availability of established methods to quantify the economic value of the insured's loss information and a general unwillingness on the part of companies to share such information. The interconnectivity of IT systems hinders the ability to measure and monitor an insurer's cyber risk exposure accumulation because a cyber-attack can trigger several insurance products and independent policies in a chain mechanism, similar to contingent business interruption.

Considering the above limitations together with the emergence of GDPR as well as the increasing numbers and ferocity of cyber threats, in this paper we propose an ICT-based framework and a comprehensive cost-driven methodology named as RiSKi for: (i) estimating cyber risks considering a quantitative approach that includes the notion of metrics and focuses on both technical and non-technical aspects, (i.e., users behaviour), that influence cyber exposure; (ii) providing analysis for efficient and effective risk management by recommending optimal investments in cyber security solutions and control; and (iii) determining the residual risks as well as estimating the insurance premiums taking into account the insurer's policy, while eliminating the information asymmetry between the insured and insurer. The proposed framework can provide services to small, medium and larger enterprises that wish to estimate and manage their risks of exposure regarding cyber threats, under the framework of the new GDPR, using a cost-benefit, quantitative approach. In addition, insurers that require to estimate the actual cost of premium using a formal and verifiable methodology that minimizes information asymmetry can apply the methodology of RiSKi.

The rest of the paper is structured as follows. Section 2 describes the RiSKi framework and its components. Section 3 provides an evaluation of the proposed RiSKi highlighting its advantages and drawbacks. Section 4 presents the related work and the added value of RiSKi, and, finally section 5 contains the conclusions.

2 THE RiSKi FRAMEWORK

Before analyzing the components of RiSKi, we first provide some definitions of the most frequently terms used throughout the paper to facilitate the better understanding of the presented notions. In cyber security, cyber risk insurance covers the cost of restoring loss to business income or reputation caused by damage to computers and computer networks. On the other hand, an insurance premium is the amount of money that an individual or business must pay for an insurance policy. Moreover, the notion of optimal investment can be explained with simple words if we consider the following question: "what is the best security measure that can be afforded given a particular budget and an associated (direct and indirect) cost?" The answer to this question is the optimal investment. Another important term is the residual risk, which is a type of risk that remains after all available security measures and tactics have been applied. Finally, it is important to mention that decisions regarding the investment and implementation or not of a particular security measure is based on the Return on Investment (ROI) analysis.

The architecture of the proposed framework is shown in figure 1. Overall, there are three distinct components: i) the Quantitative Risk Analysis Metamodel, ii) the Optimal Investment in Cyber Security, and, iii) the Symmetric Estimation of Cyber Premiums. RiSKi enhances legacy risk analysis methodologies and tools with the capability of data analytics, (either from internal or external sources) as well as security metrics related to users' behaviour, the employed technology, and the underlying environment, (i.e., malicious behaviors, social trends, economic incentives, etc.), by means of a **Quantitative Risk Analysis Metamodel**. The information carried by the latter feeds the **Optimal Investment in Cyber Security** (risk mitigation) component which: a) analyses all possible attacking scenarios and defensive strategies, (i.e., available security controls), by employing attack graphs, and b) provide recommendations for optimal investments in security controls, (i.e., technical, organizational, procedural, etc), using a set of existing econometric models and a game theory logic, while determining the residual risks. Finally, the determined residual risks together with the related attacking scenarios are used by the **Symmetric Estimation of Cyber Premiums** component that estimates the insurance premiums, taking into account also the output of the risk analysis metamodel, (i.e., users behaviors, environmental metrics, etc.), as well as the underwriter's policy, focusing on both tangible and intangible, (reputation, non-critical service disruption, etc.), assets. These steps can be repeated regularly, providing a cost-effective assessment of the cyber security investments. In the following, we analyze each of the aforementioned components of the proposed framework.

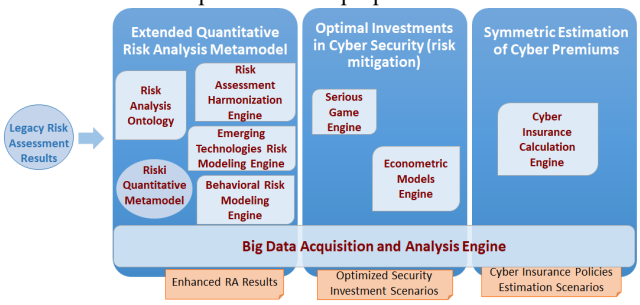

Figure 1: The architecture of the proposed RiSKi framework

2.1 Extended Quantitative Risk Analysis Metamodel

This component of RiSKi utilizes advanced security metrics in order to estimate quantitatively the exposed cyber risks, taking into account important parameters not currently considered by the existing risk analysis tools. The core part of the metamodel can be based on a well-known and widely acknowledged, free, risk analysis and management tool, like Mehari, or Verinice, which are compatible with the ISO 27005 and provide open source tools. The functionality of the selected tool is enhanced and extended in order to include and process inputs from the followings RiSKi modules:

a) A risk analysis ontology and harmonization engine that receives the outcomes of the existing risk analysis tools and harmonizes them using a common vocabulary with straightforward definition in order to be used by the proposed qualitative risk analysis metamodel.

b) An intelligent big data collection and processing engine that acquires risk related data either from internal organization sources, e.g., network infrastructure, SIEM, log files, users interaction, etc., or external sources, e.g., social media and other internet-based sources, including Darknet, using specialized crawlers. The collected and processed data will be specified and quantified within the proposed metamodel, and, thus, they will be referred to as metrics. These are:

i) Metrics on users' behaviour regarding their exposure as well as the exposure of the organization that they work for on the Internet, (i.e., social media, blogs, online service, online press, etc.), including Darknet.

ii) Metrics on users' behavior on how they use the provided infrastructure. Such metrics will be captured by developing and performing an intelligent engine that interact with users to acquire their behavior using a penetration testing approach and providing specific arithmetic results on risky actions, (i.e., specific percentage of users that open suspect files or download and execute Trojans, etc.).

iii) Metrics concerning the applied technological and procedural aspects of an organization that have direct and indirect impact on cyber security. Such metrics can be acquired by evaluating the configuration and the effectiveness of the ICT infrastructure as well as the overall organization and policies of the institution.

iv) Metrics that represent how and to what extend the external environment may threaten the underlying organization. Such metrics have to do mainly with new attack vector, malicious behavior, societal trends, political situations and economic aspects and can be acquired by developing and performing data analytics on available sources on both the visible and invisible network.

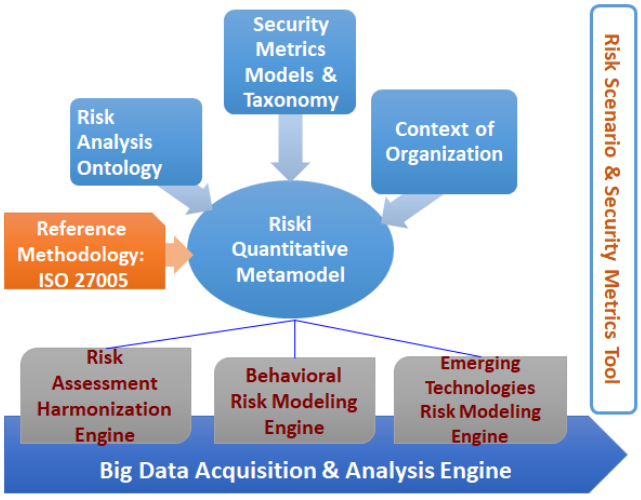

Figure 2: Big data acquisition analysis and analysis engine

2.2 Optimal Investments in Cyber Security

For the analyzing, modeling and quantifying investments in cyber security for mitigating risks, RiSKi incorporates a serious game engine as well as an engine of econometrics models for scenario planning. A serious game is a game designed for a primary purpose other than pure entertainment. The concept behind scenario planning facilitates the description of realistic stories about possible (or probable) events, based on assumptions from present trends. The purpose of scenario planning is to alert decision makers to possible outcomes of current trends and thereby to influence the decisions they make. A crucial aspect of RiSKi is to make use of the output of the quantitative risk assessment and the scenario planning approach, in order to infer additional security controls required by the business partner while meeting specific thresholds and constraints. For the selection of the optimal security controls a game theoretic approach can be followed, based on a mathematically sound method to find a way to minimize the expected damage due to an attack that exploits multiple vulnerabilities (identified or potential). To do so the first step is the identification of attack graphs based a) on the existing vulnerability reports and b) on the corporate knowledge, which are inputs from the quantitative risk analysis metamodel component. Based on these attack graphs (also known as attack trees) we upper bound for the probability that the vulnerability of a specific node is exploited (starting from any other node) by the Cumulative Vulnerability Level (CVL). Thus, the strategies of the attacker could be characterized by the path he/she uses to attack the target node. The strategies of the defender, on the other hand, are the potential actions he/she can take in order to protect his/her assets. Besides the potential countermeasures, the big data engine may provide, new, real time (or near real time) strategies that derive from the analysis of data reside at both internal and external sources to mitigate vulnerabilities. Explicitly, such strategies could be to do spot checking or patching of a vulnerable component.

Each selection of an attack and a defense strategy defines a so called scenario. In order to find an optimal solution, it must be possible to compare the consequences (payoffs) for different scenarios. In our context this payoff is the damage that occurs to the business partner. When modeling the attackers intention by choosing a target point, we implicitly describe the payoffs: if his/her intention is to attack a specific node his/her payoff is the amount of damage he/she causes there. This damage is described by the impact of exploiting vulnerability of node. Within the scope of our proposed methodology in RiSKi the payoff of the game is influenced by two factors: (a) the impact of exploitation of a single vulnerability that is measured by the impact metrics, and, (b) the level of cumulative vulnerability CVL of target node with vulnerability. Thus, the impact of an attack on a target node depends on whether the attacker is successful or not. While such uncertain payoffs yield to a somewhat more technical way of analyzing the game (see [3] for a mathematically well-founded approach to this) it does not change anything about how the game is played nor does it change the interpretation of the results the game yields. Once all strategies and corresponding payoffs are

determined, game theory yields an optimal way of choosing the actions of both attacker and defender. This equilibrium yields two piece of information: (a) how to protect the assets such that the expected damage is minimal; and (b) how likely an attacker is to choose a specific strategy, i.e. to exploit a specific vulnerability. Whenever the attacker deviates from this optimal solution he/she will end up with a worse situation that is causing less damage to the business partner.

The impact and the CVL are measured on a quantitative scale by the means of metrics for each examined scenario. Different metrics can be defined depending on the organizations' business mission, industry, and general maturity level. For example a large company with thousands of employees, a specialized security department, and a large budget for cybersecurity will have different indicators compared to a small organization that has only a few employees that must also consider sector specific regulation [4].

2.3 Symmetric Estimation of Cyber Premiums

In spite of improvements in risk protection techniques over the last decade due to hardware, software and cryptographic methodologies, it is impossible to achieve perfect/near perfect cyber-security protection [5]. In this regard, many stakeholders in the recent past have identified cyber-insurance as a potential tool for effective risk management. For cyber resilience assurance to be effective, an holistic approach like this proposed by RiSKi framework is required, which concentrates effort among ecosystem participants to develop and validate a shared, standardized cyber threat quantification framework that incorporates diverse but overlapping approaches to model cyber risk. Coverages provided by cyber-insurance policies may include first-party coverage against losses such as: a) data destruction, extortion, theft, hacking, and denial of service attacks; b) liability coverage indemnifying companies for losses to others caused, for example, by errors and omissions, failure to safeguard data, or defamation; and c) other benefits including regular security audits, post-incident public relations and investigative expenses, and criminal reward funds.

The RiSKi framework includes a component for cyber-insurance (i.e., Symmetric estimation of cyber premiums) that takes as inputs the quantitative risk assessment of an organization as well as the resulting residual risks, (i.e., after applying optimal cyber security investment procedure). This holistic approach that is followed for the assessment and estimation of the cyber insurance exposure grants the framework that enables the internalization of network and security externalities. Moreover, big data analytics supply this component with the necessary information about the internal and external company environment by providing specific values to the involved parameters and metrics. It can be widely applied to various networking domains such as organizational and enterprise networks, data centers, etc and follows a novel analytic model that enables users (i.e., companies) not to transfer the total loss recovery liability to a cyber-insurer, but may keep some liability to themselves, i.e., an Internet user may not transfer the entire risk to an insurance company. The proposed model captures the realistic scenario that Internet users could face risks from security attacks as well as from non-security related failures.

This component includes also the tasks carried by insurance carries and underwriters to estimate the insurance premiums. It is mainly a differentiated risk analysis tool that focuses on the estimation of insurance premiums by modelling cyber insurance aspects such as: a) the frequency or likelihood of loss events as well as their consequences/damages; b) the severity or insured cost of every loss event; and c) what steps of prevention and/or mitigation the company employs to either avoid (largely impossible) or reduce (definitely possible) any of the above (i.e., a or b). It will be able to assess and estimate general risk of exposure based on company industry and size, and business activities.

The component will also assess loss history, years in business and financial condition. Underwriters will inquire as to the extent of prior computer attacks. Substantial prior losses will result in an increased intensity of questioning on what steps the company has taken to reduce such losses in the future. In general, younger businesses are deemed to be more inexperienced and thus more likely to have losses than older businesses. Finally, it is important to note that this component should also evaluate the company's financial condition (balance sheet, income statement, cash flow statement).

3 DISCUSSION

The RiSKi framework extends and enhances the existing risk analysis, risk management, security investment and cyber insurance methodologies and tools with: a) big data analytics capabilities, b) users' behavior models and metrics, c) attacking scenarios and defensive strategies modeling, and d) cost benefit modeling for both security controls and insurance premiums. Big data analytics are highly relevant to cyber security, since these methods can detect patterns related to threats, disruptions and anomalies [6]. Moreover, data analytics accompanied by the proposed modeling and metrics represent a radical technological shift onto a superior technology curve compared to the state-of-the-art of human-processed.

More specifically, RiSKi implements an innovative Cyber Investment Management System that:

- incorporates detection and continuous monitoring of insiders societal behavior, to the extent permitted by the law, to proactively address anomalies and threats and their potential business impact and implications across the organization;
- provides access to published security incidents data to enable businesses to advance their understanding of cybersecurity and awareness of the threats and consequences related to cyber breaches, and, eventually, enable recovery from an event in a shorter timeframe;
- armed with the above information, employs a methodology and a supporting scenario-based cyber investment tool, for quantifying the benefits of cybersecurity investments against the many ways that potential cyber risks can affect the operation of a business;

- establishes a key role for insurers in improving the overall resilience of society to cyber risk by improving insurers' understanding about the costs associated with a cyber-event and, hence, realizing a more efficient approach to the assessment of cyber risk to traditional insurance risks.
- keeps risk analysis and management, compliance and governance frameworks in an organization up-to-date by periodically analysing the social, political, economic, and cultural dimensions of the insiders' cyber-activity, in conjunction with cyber incident data published at global scale, beyond a static compliance checklist that an organization may already have in place,
- facilitates insider risks and globally published incident data analyses to be moved up in importance and discussed in boardrooms prior to attacks, not after a significant information compromise, resulting in proactive measures to be taken to stop insider attacks from occurring, instead of reactive measures to clean up the mess,
- enables all types of organisations to provide evidence to their customers and stakeholders that appropriate risk processes related to insider threats have been applied and that up-to-date security compliance is being maintained

Using the RiSKi framework, organisations will be able to make more calculated cyber investment decisions and channel available funds to address the highest priority security needs in a proactive fashion. In particular, when properly employed, RiSKi allows organisations of all types and sizes to proactively quantify the value of cyber investments, including cyber insurance cover, produce a robust analytical framework that resonates with an organisation's strategic decisions, increase information transparency to regulatory authorities, and, eventually, operationalise the cyber capital planning process.

Another advantageous characteristic of RiSKi lies to the fact that it allows security assessments in any organization to take into account explicitly the insider factor as people merge their working and home lives while ensuring that insiders' trust and loyalty is being maintained. Also, RiSKi analytic methods can enable periodic checks and reviews on insiders' behavior as well as to cyber incident data published at global scale, hence, ensuring a proactive cyber security defense and an increased society's overall resilience to cyber-crime.

Moreover, RiSKi recognizes and promotes insurers to play a key role in improving the overall resilience to cyber risk. Cyber-insurance increases cyber-security by encouraging the adoption of best practices. Insurers can require a level of security as a precondition of coverage, and companies adopting better security practices often receive lower insurance rates. This helps companies to internalize both the benefits of good security and the costs of poor security, which in turn leads to greater investment and improvements in cyber-security.

The RiSKi Quantitative Metamodel and the Optimal Investments in Cyber Security, coupled with the Symmetric Estimation of Cyber Premiums module, can help risk management domain by establishing effective access to analytics on the social, political, economic, and cultural dimensions of the insiders' cyber-activity, as well as cyber incident data published at global scale that both support periodic and proactive cyber risk management. The successful utilisation of these inputs will, in turn, provide a platform for competitive risk assessment within an organization. The use of the RiSKi Optimal Investments in Cyber Security module will also arm the responsible executives (e.g., information security officers), with clear, justifiable, and traditional measures of financial investment, including optimal cyber insurance cover for the residual risks. In addition, knowing the financial value of prospective investment plans, as well as their alignment to the organisation's cyber value chain, the usage of Symmetric Estimation of Cyber Premiums module will enable responsible executives to conduct portfolio-level analyses that help identify the optimal set of cyber insurance policies for managing residual risks, to suit business needs.

While organisations cannot eliminate the cyber risk entirely, RiSKi will optimise cyber risk investments and help limit the economic loss and reputational impact in the event that an attack occurs. In all, with RiSKi cybersecurity scenario-based investment management platform, senior executives of all type and size organisations, including SMEs, will be able to optimise cyber security investment and cyber insurance spending, while protecting stakeholders' valued interests.

The use of the RiSKi promotes the engagement of the insurance industry in an organisation's risk assessment process by incorporating cyber insurance products to mitigate the residual risks that are in line with the organisation's cyber security strategy.

Finally it is important to mention that cyber-insurance is a relatively new area, where insurers are hampered by a lack of actuarial data with which to calculate premiums. In addition to increasing price, a lack of data leads to problems with the risk analysis undertaken by companies when deciding whether insurance against a particular risk is worthwhile. A lack of data also makes cyber-insurance appear less desirable to companies, while simultaneously increasing the price of cyber-insurance. RiSKi provides a valuable tool that address these problems, by providing an open, shared and verifiable methodology, which estimates cyber insurance exposure using a quantitative approach and metrics, considering also the risk management strategy of the organizations.

4 RELATED WORK

Recently, there is considerable joint interest from both the ICT and the economic communities in addressing the optimal investments in cyber security. The literature includes several previous works in cyber insurance but none of them propose a framework that follow a holistic approach that combines risk analysis, user behavior, and big data analytics to estimate risk and calculate cyber premiums. Anderson [7] applies economic analysis and employs the language of microeconomics (network externalities, asymmetric information, moral hazard, adverse selection, liability dumping, etc.) for explaining a number of phenomena that security researchers had previously found to be pervasive but perplexing. Also in [8], Gordon and Loeb present an economic model, referred as GL model, for determining the

optimal amount to invest for protecting a given set of information. In [9] Varian constructs a model based on economic agents' decision making on effort spent, to study systems reliability. Finally, Moitra and Konda [10] have demonstrated that as organisations start investing in information system security their protection increases rapidly, while it increases at a much slower rate as the investments reach a much higher level. A central assumption of the current GL model explicitly assumes that the probability of a cyber-breach follows a continuous evolution, leaving no room for a discrete emergence of a technological shift brought by a ground-breaking novel technology. In such a theoretical framework, the elasticity of protection of cyber security activities evades radical technological progress. Further, an implicit assumption of the GL model assumes a growing marginal cost of information security.

On the contrary to this, in RiSKi the use of big data analytics enhance the Return of Investment (ROI) in information security, and thus, a growing marginal cost of information security activities would not be acknowledged anymore. As denoted by influential practitioners, the cost of any information is expensive to produce, but cheap to reproduce. Consequently, the marginal cost of production of a given information good tends to zero. Therefore, once fixed costs of developing big data analytics would be borne, the price of (re)producing relevant security information would therefore tend to zero. This is even more compelling while information technology infrastructures operators produce and store a large amount of industrial data that are costless.

Finally, in Cyber Insurance models, in [11], the authors show that in a cyber-insurance framework, cooperation amongst network users results in the latter making better (more) self-defense investments than the case in which they would not cooperate. Thus, the authors' results reflect that cooperation amongst network users will result in a more robust cyberspace. However, not all applications in cyberspace can be cooperative and as a result we consider the general case of non-cooperative application environments and to ensure optimal insurance-driven self-defense amongst users in such environments. In another recent work [12], the authors derive Aegis, a novel optimal insurance contract type based on the traditional cyber-insurance model, in order to address the realistic scenario when both, insurable and non-insurable risks co-exist in practice. They mathematically show that: (i) for any type of single-insurer cyber-insurance market (whether offering Aegis type or traditional type contracts) to exist, a necessary condition is to make insurance mandatory for all risk-averse network users; (ii) Aegis contracts mandatorily shift more liability on to network users to self-defend their own computing systems, when compared to traditional cyber-insurance contracts; and (iii) it is rational to prefer Aegis contracts to traditional cyber-insurance contracts when an option is available. However, the authors do not analyse markets for cyber-insurance, where one needs to consider as important goals, maximizing social welfare, and satisfying multiple stake-holders. Without such considerations, simply shifting liability on users to invest more may not be enough for a successful cyber-insurance market.

The work, carried in the related literature mentioned above, considers an ideal insurance environment, i.e., where there is no information asymmetry between the insurer and the insured. In RiSKi, it is tried to eliminate information asymmetry, but not by taking into account an unrealistic assumption; on the contrary by applying and a verifiable and shared methodology that includes standard and enhanced procedures: quantitative risk analysis using security metrics derived by internal and external factors (vulnerabilities, user behavior, etc.) as well as optimal security investments for managing cyber risk. Moreover, when required, game theory can be activated to assist in decision making. RiSKi framework also considers interdependent and correlated risks, inherent in computer systems and networks, by including the steps of quantitative risk analysis and using attack graphs.

5 CONCLUSIONS

This paper proposed a cyber investment management framework named RiSKi that incorporates detection and continuous monitoring of insiders societal behavior, to the extent permitted by the law, to proactively address implied anomalies and threats and their potential business impact and risks. Moreover, using a web crawler it provides access to published security incidents data to enable businesses to advance their understanding of cybersecurity and awareness of the threats and consequences related to cyber breaches, and, eventually, enable faster recovery from an event. RiSKI armed with the above information, employs a methodology, and develops a supporting scenario-based cyber investment calculation tool.

ACKNOWLEDGMENTS

This research has been funded by the European Commission as part of the ReCRED project (Horizon H2020 Framework Programme of the European Union under GA number 653417).

REFERENCES

[1] ISTR, Internet Security Threat Report, Symantec, Vol. 22, April 2017.
[2] ENISA, Cybersecurity as an Economic Enabler, March 2016.
[3] O.H. Alhazmi, Y.K. Malaiya, and I. Ray. 2007. Measuring, analyzing and predicting security vulnerabilities in software systems. Computer Security, Elsevier, 26, 3, 219–228, 2007.
[4] NIST SP 800-55, "Performance Measurement Guide for Information Security", http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf
[5] LondonAssembly, Police and Crime Committee, "Tightening the net The Metropolitan Police Service's response to online theft and fraud", March 2015
[6] Mayer-Schönberger and K. Cukier, "Big Data: A Revolution that Will Transform how We Live, Work, and Think", Houghton Mifflin Harcourt
[7] R. Anderson, C. Barton, R. Böhme, R. Clayton, M.J. Van Eeten, M. Levi, T. Moore, and S. Savage. "Measuring the cost of cybercrime", Econ. Inf. Secur. Priv., Springer, pp. 265–300, 2013
[8] L.A. Gordon and M.P. Loeb, "The economics of information security investment", ACM Transactions on Information System Security, (TISSEC), 5(4), 438–457, 2002.
[9] H. Varian, "Fifth International Conference on Electronic Commerce (ICEC), ACM, 2003, pp. 355–366
[10] S. Moitra, S. Konda, "The survivability of network systems: An empirical analysis", Carnegie Mellon Software Engineering Institute, Technical Report, CMU/SEI-200-TR-021.
[11] R. Pal and L. Golubchik, "Analyzing self-defense investments in the internet under cyber-insurance coverage", In IEEE International Conference on Distributed Computing Systems (ICDCS), 2010
[12] R. Pal, L. Golubchik, and K. Psounis. "Aegis: A novel cyber-insurance model" IEEE/ACM GameSec, 2011.