Aviad, Adiel; Weçel, Krzysztof; Abramowicz, Witold

Article

A concept for ontology-based value of cybersecurity knowledge

International Journal of Management and Economics

Provided in Cooperation with:
SGH Warsaw School of Economics, Warsaw

Suggested Citation: Aviad, Adiel; Weçel, Krzysztof; Abramowicz, Witold (2018) : A concept for ontology-based value of cybersecurity knowledge, International Journal of Management and Economics, ISSN 2543-5361, De Gruyter Open, Warsaw, Vol. 54, Iss. 1, pp. 50-57, https://doi.org/10.2478/ijme-2018-0005

This Version is available at:
https://hdl.handle.net/10419/309655

Research Article

Adiel Aviad, Krzysztof Węcel*, Witold Abramowicz

A Concept for Ontology-Based Value of Cybersecurity Knowledge

https://doi.org/10.2478/ijme-2018-0005
Received June 9, 2016; accepted February 3, 2018

Abstract: This paper focuses on cybersecurity knowledge, claiming that this knowledge may have a value of its own, and suggests a market mechanism to foster the creation of this kind of value. The goal is to elaborate the value of cybersecurity knowledge and propose a semantic approach with an example model to enable better handling of the relevant body of knowledge and its value. The problem of attributing value to cybersecurity should be perceived as analogous to that in information technology. We have examined the relevant body of knowledge with a focus on its characteristics from the viewpoint of different types of market players and their interests. By applying our model, it is possible to increase the accessibility of knowledge and observe externalities from sharing thereof.

Keywords: cybersecurity, threats, value, Semantic Web

JEL codes: D46, D62, D89

1 Introduction

Cybersecurity is the sum of the effort and steps taken to prevent the deliberate use of an information system in a way not intended by the system owners. It is very often considered by an enterprise as an investment that needs to be justified, i.e., it should yield the expected economic results. In general, it is difficult to assign value to information technology (IT), and a similar challenge concerns cybersecurity tools too. In this paper, we focus on treating cybersecurity knowledge as a subject with value of its own.

This paper aims to propose a market mechanism for the handling and valuation of the body of knowledge on cybersecurity. Such a mechanism should facilitate the creation of value for such knowledge. The proposed solution is to adopt a semantic approach, expecting an increase in value through the process of making the knowledge more useful in terms of accessibility, automatic processing, and sharing.

The paper is organized as follows. First, related work is presented, together with relevant concepts, including market forces. The global perspective is taken, considering all types of market players. The need for a proper market mechanism to add value to this knowledge is identified. The Semantic Web technology is presented, and the suitability of the semantic approach to the domain of cybersecurity knowledge is elaborated. A semantic market mechanism is proposed, enabling the assigning of values to all parts of the body of knowledge on cybersecurity. Finally, creation of value through the proposed mechanism is exemplified.

***Corresponding author: Krzysztof Węcel,** Poznan University of Economics, Poznan, Poland, E-mail: krzysztof.wecel@ue.poznan.pl
Adiel Aviad, Witold Abramowicz, Poznan University of Economics, Poznan, Poland

2 Background and Related Work

We consider the concept of value in two senses. One is the sense of value as defined by Barney [1991]: a firm's resource is considered valuable if it "exploits opportunities and/or neutralizes threats in a firm's environment". In the context of cybersecurity, the value may be for a community of defenders ("well-behaving" organizations), relative to attackers. This is indeed a change from the common context of competition, yet it is another kind of competition as cyber threat agents may be considered risks that behave like a kind of competition with rival market players. The term "value" here is meant to quantify the benefit that such knowledge may bring to those who may use it. Using it may involve either consuming the knowledge or identifying missing knowledge to be added.

Another sense of value that we consider is the shared value. Companies can create economic value by creating societal value [Porter and Kramer, 2011] in three ways: reconceiving products and markets, redefining productivity in the value chain, and building supportive industry clusters. Having a well-managed, accessible, and shared body of cybersecurity knowledge may clearly follow the first and the third ways of creating such value. It also supports corporate social responsibility by providing such knowledge to the society. This kind of benefit to society is in a way that is appropriate to a firm's strategy and is not standardized for all companies, which is more productive [Porter and Kramer, 2006]. In recent years, creating shared value has become an imperative for corporations [Kramer and Pfitzer, 2016], and shared knowledge supports shared value.

The contribution of IT to value creation is subject to the modern productive paradox. Cybersecurity is a part of IT, and cybersecurity knowledge is a part of cybersecurity. In a previous study [Magnusson et al., 2007], value creation by investment in security is examined in an enterprise context. The "modern productive paradox" [David, 1990] is mentioned as a reason for the difficulty in justifying IT security investments like for other IT investments in general, as well as several other reasons. Three models of return on security investments (ROSI) are presented: the Hummer model [Wei et al., 2001], the Hoover model [Sudbury et al., 2001], and the Carnegie Mellon University (CMU) model [Moitra and Konda, 2000]. Their applicability in value creation is discussed, and the authors conclude that "it is neither easy to verify whether the models claim to be economically correct, nor if they claim to develop a valuation model for ex post or ex ante perspective". Three companies are then examined, but none had any knowledge of the three ROSI models or any other method, nor any evidence of shareholder value perspective on IT security. In our view, all these considerations reflect a problem that causes enterprises to not consider cybersecurity as a subject for value creation. Works such as that by Gordon et al. [2003] address this issue through an insurance viewpoint of an organization's assets and risk assessment. Other works [e.g., Ben Aissa et al., 2010] suggest a quantitative way to estimate the cost of security threats through the potential damage to stakeholders. These works consider only the viewpoint of an enterprise, apart from considering only the security measures as a whole, with no value for the knowledge itself. However, there is value for the security knowledge itself, and Miller [2007] provides the estimates of various kinds of vulnerabilities, and their worth ranges from $500 to $250,000.

A good economic perspective on the cybersecurity market (although not the cybersecurity knowledge market) is provided by Anderson and Anderson [2001], suggesting an explanation of this market using economical concepts: Asymmetric information or the "lemon" effect [Akerlof, 1970] is the lack of sufficient buyer information, which presses down prices of products since the buyer cannot make a distinction between highly secured products and poorly secured ones. The concept of dumping of liability or "tragedy of the commons" [Hardin, 2006] implies that owners of assets would not make any effort to avoid their assets being used by attackers (e.g., to serve in a denial-of-service attack) as the corresponding cost would be higher than their part of the damage caused. Network economy and network externalities are presented in the study by Shapiro and Varian [1999] and explain why vendors try to get the largest market share as soon as possible, neglecting security aspects.

In a previous study [Böhme, 2005], five possible models for the vulnerabilities market are presented: bug challenges, bug auctions, vulnerability brokers, exploit derivatives, and cyber insurance. The approach we present in this paper is about handling the body of knowledge on cybersecurity and is capable of supporting all these models.

These market models are judged by the following four criteria: (1) information function aims to counter the "lemon effect" by the ability to use market prices as forward-looking indicators for security properties; (2) incentive function involves compensation for security research-and-development in order to motivate firms and individuals to give security a higher priority; (3) risk-balancing function is the provision of instruments to hedge against large information security risks; and (4) the fourth criterion is the efficiency of the market model.

Our approach here refers to improving knowledge sharing, and therefore, it certainly counters the "lemon effect". It also provides a means for the market players to demarcate and "bid" for missing pieces of knowledge – providing incentives for security researchers to make the effort and create this missing knowledge. Proper use of the proposed mechanism may also assist organizations in identifying and eliminating the detected security risks and to identify such risks even better in the future [Aviad et al., 2016].

3 Market Mechanisms for Value in Cybersecurity

In this paper, we refer only to the knowledge part of cybersecurity, but in a global context, which is wide enough to include not only enterprises but all market players such as vendors seeking to improve their products, individuals (e.g., security experts) looking for opportunities to make a contribution, consulting services, and other organizations, in addition to enterprises. Cybersecurity knowledge parts may be considered products in their own right, having their own value. Each knowledge item, or collection of items, may have a value for some of the market players. Even an "empty" item of knowledge (e.g., identification of a required mitigation) may have a value by recognizing missing knowledge that is required. Some of these knowledge products are tightly related to other products, such as hardware or software to which they are applicable, while others may have value as independent products that provide solutions such as general mitigations (e.g., properly validating an input). The relations with other knowledge items can also be valued, such as a relationship between a threat and a hardware or software item to which the threat is applicable. All of these products/knowledge items are related to other knowledge items, creating a "fabric of knowledge". These knowledge products are delivered and consumed by various market players as elaborated in the following sections. We suggest a market mechanism that may provide further valuation to the market. We consider security knowledge as goods with value of their own and not as components only, conditioned by the other commercial activities of the main services or products. Such a mechanism may counter the lemon effect and separate the aggregate value of the knowledge to many market players on the one hand from the cost of creating that knowledge on the other.

The mechanism we propose supports the assignment of value and management of the knowledge in a way that lends itself to many desired views and players. It also encourages sharing of knowledge so that the value of whole views is greater than the sum of their knowledge parts.

The market of cybersecurity may be characterized as a knowledge-intensive business service (KIBS), due to the expertise and knowledge required for offering services. We propose creation of a fabric of cybersecurity knowledge (existing or desired knowledge). Considering only the knowledge and excluding the goods makes this market to be a less goods-dominant (G-D) and more service-dominant (S-D) one. Much of the knowledge items refer to goods/products and foster supplier–customer interaction by identifying flaws in products, then creating products to compensate for the flaws, and so on. This kind of knowledge does not exist up-front (in this case, it is embedded in the design of hardware or software goods) but rather is discovered and added gradually later, when security deficiencies are discovered and cures are devised. This is an ongoing process rather than a one-time offering of goods. Such fabric of knowledge also enables the identification of desired knowledge (e.g., how to cope with flaws), thus encouraging supplier–customer cooperation in identifying vulnerabilities and finding mitigations.

The suggested mechanism may provide not only knowledge but also serve as a channel of communication between customers and providers, as well as among peers of all kinds. In another study [Lusch, 2006], there is emphasis on the "central role of networks and interaction in value creation and exchange". The suggested mechanism may provide such a network and thus enable efficient interaction. In addition, the notion of

co-creation of value during product use as a "rather drastic departure from G-D logic" is stated. The authors explain that value is added with the user during the consumption process rather than during production, while the goods comprise the "distribution mechanism for service provision". With our suggested mechanism, a significant part of the knowledge will be created with the users (as the "operant resources" of S-D logic), pointing out the required knowledge and implementing it when added, while having the hardware/software products serve as the distribution mechanism – to which the desired knowledge refers and to which added knowledge is applied. Therefore, the suggested mechanism is expected to encourage the market behavior to be more S-D oriented rather than entail G-D logic.

4 Sources of Value, Network Effects, and Externalities

Enterprises may perceive the value of cybersecurity in several ways. In the study by Magnusson et al. [2007], the following are identified: saving the cost of cyber attack damage, saving the cost of manual security processes, and enabling business services that would not be sustainable without cybersecurity. In addition, improved cybersecurity may provide the enterprise with a competitive edge over enterprises that consumers perceive as less secured.

For integrators, such knowledge may ease and improve the security aspect of their work and enable the higher-value outcome for their customers. The possibility of revealing their "trade secrets" should not be of major impact as this kind of knowledge is usually not a commercial asset for integrators.

For vendors that manufacture commercial off-the-shelf (COTS) tools for cybersecurity, the revenue comes from selling and supporting their products. Such products may be either general-purpose "payload" technology or defense products. The difference in the purpose of the product may influence the manner of quantifying the value, since for general-purpose products, the value may be perceived by analogy to insurance premiums, while for defense products, the value is in the essence of the product. However, in both cases, cybersecurity adds value to the product or the services.

The dynamic, complex, and scattered nature of cybersecurity requires efforts to make the relevant body of knowledge a prominent enabler for cybersecurity, thus creating value in cybersecurity knowledge. Intelligent risk assessment should consider the nature of threats. Knowledge is needed to determine and prioritize threats and countermeasures. Creation and utilization of the knowledge is done by individuals, enterprises, vendors, and state agencies.

Cybersecurity knowledge does not carry a network effect, as a consumer does not get any benefit from others consuming that knowledge (for vendors, this may even increase competition). Yet, there is a positive externality of having a better, more-secure environment by reducing infections by viruses if other enterprises consume the same knowledge (for vendors, this is of minor importance). Moreover, attacks carried out by an attacker by controlling "innocent" computers (i.e., distributed denial-of-service attacks) would be reduced if attackers would not get so many computers under their control. The case of Advanced Persistent Threat (APT) – where the attacker targets a specific target for a long time – is an exception, but the general case is of having a better environment for all. Once again, for vendors, the case is different as they focus on products and are less sensitive to the environment. This externality may imply that there is a justification for some intervention by governments or global organizations, since the overall benefit of a better-secured environment is higher than the benefit for a single consumer. Therefore, the desired market equilibrium should be based on having more and better security knowledge than the equilibrium that would satisfy a single consumer, who would tend to research less and be satisfied with less security knowledge. In fact, agencies and organizations such as MITRE, National Institute of Standards and Technology (NIST), and Open Web Application Security Project (OWASP) are already active in this field.

Cybersecurity knowledge requires a high level of expertise over a wide range of technological disciplines, together with traits of creativity, dedication, and other characteristics of highly skilled personnel. The costs of such personnel are the main reason why this is a case for economy of scale. Indeed, there are a lot of individual contributors of cybersecurity knowledge, such as researchers and hackers, but they usually do this not for profit but for prestige. The prestige is important not only for researchers but also for hackers,

as this is a discipline with no certifications, and achievements are the way to gain recognition. Individual contributions usually involve finding breaches in a certain technology or environment, while cybersecurity requires mastering the full range of technologies in use in order to secure all possible breaches. The expenditure on retaining such expertise and the required infrastructure is fixed in nature, implying significant advantages for economy of scale. If the benefits of such security knowledge could be shared, then the burden of cost could be lighter. This requires attribution of value to cybersecurity knowledge.

5 Added Value of Cyber Threat Intelligence

Having presented the value of cybersecurity, it is worthwhile to point out the value of cyber threat intelligence. Cyber threat intelligence, in addition to the above-mentioned reasons for sharing, entails another feature: the whole is bigger than the sum of its parts, as items must be connected in order to get insights. It seems that it has already been recognized how important it is to have the relevant knowledge shared, to build an integrated "big picture", and extract better insights. The USA Cyber Threat Intelligence Integration Center (CTIIC) was established in 2015 as a federal agency meant to be "a fusion center between existing agencies and the private sector" [Aliya Sternstein, 2015], focusing on "connecting the dots" [The White House, Secretary, no date (n.d.)]. The Cyber Intelligence Sharing and Protection Act (CISPA) is a US-proposed law, which allows for the "sharing of certain cyber threat intelligence and cyber threat information" [Permanent Select Committee on Intelligence, 2012]. At the technical level, the Structured Threat Information Expression (STIX) language was developed to standardize information about cyber threats [Barnum, 2014]. Standards may be seen as enablers for cooperation and sharing of information. These three are examples that indicate an increasing awareness of the importance of cooperation and the sharing of efforts regarding cyber threat intelligence.

6 Semantic Technologies for Knowledge Organization

The vision of the Semantic Web, as presented by Berners-Lee et al. [2001], points to ontology as the third and most advanced pillar of knowledge organization. Ontology provides the means to create taxonomy of concepts, relationships, and inference rules, in addition to serialization formats such as Extensible Markup Language XML and Resource Description Framework RDF, which provide structure and "local" meaning, respectively (that is not communicated across the above-mentioned boundaries). As the World Wide Web Consortium (W3C) states, "The Semantic Web provides a common framework that allows data to be shared and reused across application, enterprise, and community boundaries" [W3C, n.d.].

The Semantic Web technology may provide a mechanism that supports attribution of value to varying pieces of knowledge. Furthermore, it may provide a mechanism for global crowdsourcing, in addition to enabling individual contributions. Basic content sharing over the Web is enabled by the design, but the Semantic Web enables more intelligent sharing by both humans and applications using ontologies. This requires handling of the meanings of pieces of the contents (concepts) and the relationships between such concepts.

Ontology enables the Semantic Web to bridge over the differences in terminology and meaning that apply in a community such as the diverse and scattered community of the cybersecurity. The classifying mechanism of concepts provides a way to express the "family" nature of cyber threats, IT assets, attack vectors, and countermeasures. Concepts representing such entities are characterized by their origin from a base form in accordance with the "carrying" technology. This means that concepts representing such entities may be handled by subclassifying them from a common superclass. Rules enable reasoning of new facts, based on already-known facts.

Ontology of cybersecurity knowledge may provide a market platform for this knowledge. Pieces of knowledge may be demarcated – from a single concept as a threat or countermeasure, to a facet of the ontology that pertains to a specific technology, to the entire ontology. Each such piece of knowledge may (optionally) be assigned a price tag; however, larger facets would be more useful, such as all existing vulnerabilities

and countermeasures that apply to a certain technology, vendor, or product, providing a sound base for its valuation, in addition to serving commerce. Such a price may be assigned for already-existing knowledge or for knowledge that does not exist yet, e.g., a solution sought for a known vulnerability – as priced by the requesting enterprise or several enterprises, reflecting its value for the intended buyers. In a case like this, the aggregate value of several offers, submitted by a number of enterprises in need, may bring experts to conduct a research and find a solution that otherwise would not cover the cost of the research. Vendors may see this as an indication for the more painful (and of higher value) problems. Such a market may include future contracts and options similar to other markets. The prominent difference from other markets is that knowledge goods may be sold several times to several buyers or be requested several times by interested buyers although it does not exist yet. Such a market may resemble a music market, except the dimension of future – future music may not be defined and demarcated as a vulnerability, countermeasure, and so on. The suggested market may be characterized as a knowledge market that is part of the knowledge economy.

The proposed market mechanism may support various models of consumption by subscription, by pay per answer, or by the trading of pieces of knowledge (monetization). The latter encourages cross-specialization, wherein one organization specializes in cybersecurity knowledge that pertains to its core business, such as threats to specific machinery or health equipment, and trades it with a partner for cyber knowledge regarding systems of secondary importance such as general-purpose IT.

7 Proposed Semantic Security Model

The Semantic Web, as defined by Shadbolt et al. [2006], is indeed a technology that includes important features to accommodate the cybersecurity knowledge: the ontology to specify and organize all entities and relationships; the rules to reason new knowledge; the classes and subclasses to capture the "family" nature of threats and the richness of varieties; the capability to semantically bridge over terminology variations; and the capability of sharing content all over the Web to enable everybody to access the knowledge. Yet, a market must secure both the goods and the transactions.

Securing the goods can be implemented by separating the text parts from the concepts and storing them in a file system or a database subject to access control, with the properties of the concepts serving as the metadata identifying this particular piece of knowledge. Common technologies may also secure the transactions, handling authentication of users, authorization, nonrepudiation, information integrity, and confidentiality, like any other transaction. Data on the move (in transaction) may be encrypted asymmetrically using a private key for each consumer.

Securing the transactions depends on the monetization model but can also be done using common technologies. The Semantic Web has several evolving ways to support security, from secured Web services to XML encryption. This may enable automatic computer software to consume the knowledge, but this is beyond the scope of this work.

8 Example Value-Creation Scenarios

Let us consider a hacker who finds a product defect and publishes it (i.e., an exploit) for free, gaining the appreciation of a hacker society. This way he may get a wider exposure and a higher value for the effort – so he may do further work of this kind, to the common "benefit" of the entire community.

An enterprise that uses this product has a cyberinsurance in case a cyberattack causes a denial of business service or leakage of customer information. However, the insurance company is expected to raise the premium for enterprises that have such unmitigated vulnerabilities. The enterprise has to consider replacing the product to avoid the premium raise.

Help can be expected from a security vendor who publishes a configuration for its security product. Its customers can set up their products to work with improved configuration – an alert can be raised in the case of an attack. The enterprise has this security product installed in its environment, so it devises a mitigation that is based on such an alert followed by a manual procedure. The raise of the insurance premium can

thus be avoided. The value of the security product is increased – for the enterprise, for the vendor, and all customers.

Vendors that make use of the defective product or technology (e.g., a protocol) in their own products also observe this. Possibly, they could note this through an automatic mechanism that monitors all their products for the discovery of new defects. Semantic inference may be used to reason about the defects of infrastructure products so that other products that are based on these infrastructure products can avoid problems.

Two further scenarios for threat handling can be distinguished. One product vendor publishes a bypass through a secure setup in the form of a new product – this raises the product's value, but for the enterprise, it means replacing the product it already owns and uses. Such a replacement involves costs, and the management prefers to avoid it, so they keep using the old product with the alert from the security product and the manual procedure that follows each alert. Another product vendor publishes a solution – a new version of its product. This is the product that is in use by the considered enterprise, so it upgrades the product version and gives up the manual procedure.

The above-described scenarios involve cybersecurity concepts such as attack patterns, exploits, mitigations, and vulnerabilities, as well as their relationships. These concepts and relationships are included in the proposed model and may be processed even automatically so that all the mentioned players are provided with the knowledge they need. This can be done using preprepared queries that monitor the body of knowledge for new relevant knowledge. Each player may use the query that fits his needs, e.g., the hacker contributes a description of the vulnerability and relates it to the product, the enterprise queries for vulnerabilities of its assets, vendors query for opportunities in their area of expertise and contribute mitigations, and so on. The players become more knowledgeable, and the market becomes more perfect (in terms of knowledge). The body of knowledge expands and even more value is created.

9 Discussion and Conclusions

The semantic approach to handling the body of knowledge on cybersecurity encourages creation of value for this knowledge and makes it more shared and accessible. Adding a new knowledge item, e.g., a new threat, not only improves security in general but also creates business opportunities for various kinds of entities: security vendors, administrators, and integrators. A market mechanism such as the suggested one encourages this creation of value by sharing the benefits and expedites the creation of value by mechanizing it. Such a mechanism also promotes the benefits of economy of scale by augmenting a lot of sources in parallel and makes the market and the competition more perfect through sharing of knowledge. The activity in this field as of today implies that due to externalities, there is a place for some intervention from governments or international organizations.

In this work, we suggest that cybersecurity knowledge may be considered to have value by itself, to make it shared and accessible through the semantic approach, and make it a relevant, implementable model. We have described how this would enable better valuation of this knowledge and improve security.

We have not provided a mechanism for the trading of knowledge but for the handling and valuation of it. A safe trading mechanism still requires further work, considering the various types of market players as well as the various views and parts of knowledge that might be requested. The body of knowledge relevant for cybersecurity is a prominent part of cybersecurity as a whole. Handling it as a good in its own right through a dedicated mechanism would give it a more appropriate value and better overall security as a result.

References

Aviad, A.E., Węcel, K., Abramowicz, W. (2016), A semantic approach to modelling of cybersecurity domain, *Journal of Information Warfare*, Vol. 15, No. 1, pp. 91-102. Available at: http://www.jstor.org/stable/10.5325/jinfopoli.1.2011.0001.

Akerlof, G.A. (1970), The Market for "Lemons": quality Uncertainty and the Market Mechanism, *Quarterly Journal of Economics*, Vol. 84, No. 3, pp. 488-500.

Aliya Sternstein. (2015), Obama's New Cyber Agency Puts Spies in Charge of Sharing Threat Tips with Agencies, *Nextgov*. Available at: http://www.nextgov.com/cybersecurity/2015/02/obama-creates-cyber-cia-or-obama-creates-cyber-counterterrorism-center/105051/ [Accessed May 22, 2016].

Anderson, R., Anderson, R. (2001), Why Information Security is Hard, *Annual Computer Security Applications Conference*. Available at: www.cl.cam.ac.uk/~rja14/#Econ.

Barney, J. (1991), Firm resources and sustained competitive advantage, *Journal of Management*, Vol. 17, No. 1, pp. 99-120. Available at: http://jom.sagepub.com/cgi/doi/10.1177/014920639101700108.

Barnum, S. (2014), STIX Whitepaper. Available at: http://stixproject.github.io/getting-started/whitepaper [Accessed December 23, 2015].

Ben Aissa, A., Abercrombie, R.K., Sheldon, F.T., Mili, A. (2010), Quantifying security threats and their potential impacts: a case study, *Innovations in Systems and Software Engineering*, Vol. 6, No. 4, pp. 269-281.

Berners-lee, T.I.M., Hendler, J., Lassila, O.R.A. (2001), The Semantic Web, *Scientific American*, Vol. 284(May), pp. 1-4. Available at: http://www.nature.com/doifinder/10.1038/scientificamerican0501-34.

Böhme, R. (2005), Vulnerability markets what is the economic value of a zero-day exploit? In *Chaos Communication Congress*, (December), pp. 27-30. Available at: https://events.ccc.de/congress/2005/fahrplan/attachments/542-Boehme2005_22C3_VulnerabilityMarkets.pdf.

David, P.A. (1990), The Dynamo and the Computer: an Historical Perspective on the Modern Productivity Paradox, *American Economic Review*.

Gordon, L., Loeb, M.P., Sohail, T. (2003), A Framework for using insurance for cyber-risk management, *Communications of the ACM*, Vol. 46, No. 3, pp. 81-85.

Hardin, J.G. (2006), The tragedy of the commons, *Environmental Issues: Essential Primary Sources*, Vol. 162, December, pp. 64-68. Available at: http://find.galegroup.com/gic/infomark.do?&source=gale&idigest=0f0174f8fbc32fe7c817214d754d9f0e&prodId=GIC&userGroupName=c_gic&tabID=T0011&docId=CX3456400036&type=retrieve&contentSet=EBKS&version=1.0.

Kramer, M.R., Pfitzer, M.W. (2016), The ecosystem of shared value, *Harvard Business Review*, October, pp. 1-11. Available at: http://www.fsg.org/publications/ecosystem-shared-value?utm_source=fsg&utm_medium=email&utm_campaign=201609ecosystemofsharedvalue#download-area.

Lusch, R.F. (2006), Service-dominant logic: reactions, reflections and refinements, *Marketing Theory*, Vol. 6, No. 3, pp. 281-288.

Magnusson, C., Molvidsson, J., Zetterqvist, S. (2007), Value creation and return on security investments (ROSI), *IFIP International Federation for Information Processing*, Vol. 232, pp. 25-35.

Miller, C. (2007), The Legitimate Vulnerability Market Inside the Secretive World of 0-day Exploit Sales. In *Workshop on the Economics of Information Security, Pittsburgh, PA*. pp. 1-10. Available at: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.139.5718.

Moitra, S. D., & Konda, S. L. (2000). *A simulation model for managing survivability of networked information systems* (No. CMU/SEI-2000-TR-021). CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

Permanent Select Committee on Intelligence. (2012), *Cyber Intelligence Sharing and Protection Act Report together with Minority Views to Accompany H.R. 3523*, Available at: http://www.gpo.gov/fdsys/pkg/CRPT-112hrpt445/pdf/CRPT-112hrpt445.pdf.

Porter, M.E., Kramer, M.R. (2006), Strategy & society, *Harvard Business Review*, 84, December, pp. 78-92.

Porter, M.E., Kramer, M.R. (2011), Creating shared value, *Harvard Business Review*, Vol. 89, No. 1-2.

Shadbolt, N., Berners-Lee, T., Hall, W. (2006), The semantic web revisited, *IEEE Intelligent Systems*, Vol. 21, No. 3, pp. 96-101. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1637364.

Shapiro, C., Varian, H. R., Becker, W. E. (1999). *Information rules: a strategic guide to the network economy*. Journal of Economic Education, 30, 189-190.

Soo Hoo, K., Sudbury, A.W., Jaquith, A.R. (2001), Tangible ROI through secure software engineering, *Secure Business Quarterly*, Vol. 1, No. 2.

The White House & Secretary, Office of the Press. (2015), Cyber Threat Intelligence Integration Center. Available at: https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center<http://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center> [Accessed May 19, 2016].

W3C. (n.d.), What is the Semantic Web. *W3C Semantic Web Activity*. Available at: http://www.w3.org/2001/sw/[Accessed August 16, 2015].

Wei, H., Frinke, D., Carter, O., Ritter, C. (2001), Cost-benefit analysis for network intrusion detection systems. In *CSI 28th Annual Computer Security Conference*. pp. 29-31.