Economic Benefits of Value-Based Approaches to Computer Security Assurance Over Compliance-Based Approaches

Chris Henk
40252177
cahenk@smu.edu

***Abstract*— In this paper, we demonstrate the increased efficacy of value-based approaches to computer security assurance over those that are compliance-based. As the reliance of organizations on their IT infrastructure to conduct business grows, so too does the threat posed by inadequate security programs. Compliance-based approaches are value-neutral and are unable to produce quantifiable metrics, which promotes malinvestment and inhibits effective communication with C-level executives. A survey of the literature on value-neutral approaches is provided to highlight the systematic issues inherit to them. We introduce a novel analysis of value-neutral approaches that includes compliance-based approaches to demonstrate that being compliant is not the same as being secure. Furthermore, we perform a case study of the security firm Armor to prove veracity of these claims. Our case study demonstrates that security outcomes can improve by more than an order of magnitude, while delivering an ROI of up to 286% by implementing value-based approaches. We conclude that the economic and managerial concerns of compliance-based, value-neutral approaches can be resolved by employing a value-based approach instead.**

I. Introduction

The criticality of an organization's ability to perform computer security assurance has never been more apparent. As the march of technological capacity drives forward and costs decline, organizations become increasingly reliant on their IT infrastructure. With hundreds of billions of dollars worth of assets at stake, a wide range of criminal, governmental, and corporate threat actors of ever increasing sophistication have emerged. It is paramount that the sophistication of the methodologies meant to combat these actors scale with the severity of the threat.

Despite the reality that cyber threats have never been more serious or prolific, security assurance methodologies have failed to reflect adapt. Most firms today implement what is best described as compliance-based security, where the organization does the bear minimum to comply with the requirements placed upon them by regulatory agencies and/or as a condition of doing business with third party partners. Being compliant is not the same as being secure. Compliance is value-neutral and unable to accommodate the specific needs of the organization to achieve optimal economic and security outcomes. This is because value-neutral approaches to security are not effective at conveying their business case and therefor seldom receive the necessary level of funding and attention. Additionally, it provides no clear way to measure ROI because quantifiable metrics cannot be produced to measure the outcome of each security investment [1].

Further clouding the return on security investment is that it is measured in terms of losses avoided rather than in terms of revenues generated. This makes security investment more akin to purchasing insurance than it is to making capital expenditures in increasing capacity, for instance. These factors act as problematic barriers to effectively communicating with C-level executives leads to insufficient security funding and ensures that a substantial portion of what limited funding is available will be grossly gross misallocation [2]. Additionally, their one size fits all approach to security leads resources to be misappropriated by funding activities that do not improve the organization's security posture [3]. Hence compliance is typically the only facet of security assurance that is properly funded because the regulatory burden placed on the company is the business argument for doing it. Value-based approaches go beyond compliance to enable security. By considering the specific financial outcomes that result of the different risks facing an organization's assets, value-based approaches demonstrate their investment justification in a clear, quantifiable way with the added benefit of allocating resources more efficiently by maximizing the measured value [4].

In this paper we demonstrate the clear issues with value neutral approaches and how implementing a value-based approach can address both the concerns of ineffective communication with C-level executives, and therefore minimal investment, and how what resources are available can be managed and allocated to achieve substantial economic outcomes. We introduce a novel analysis of the efficacy of value-based approaches with a case study of the security firm Armor that demonstrates the difference between compliance and security. Our results show that replacing a compliance-based approaches with value-based ones can improve security outcomes, some by a factor as high as 100, and that the resulting security investment can yield an ROI of up to 286% over an existing compliance-based implementation.

The need for improved security paradigms is growing each day. Most organizations today are not rising to meet emerging

threats because they follow compliance-based approaches to computer security assurance that promote a variety of issues such as improper funding levels, malinvestment, and managerial challenges. Value-based approaches correct these concerns by producing quantifiable metrics for security investment-outcome pairs. This data allows for ROI to be determined, continuous improvement to be implemented, and for the business case of investments to be clearly and easily conveyed to C-level executives. We conclude that organizations must undergo this paradigm shift at the earliest opportunity, and that the longer they wait the greater the chances of a catastrophic security breach become.

The remainder of this paper is organized as follows. In Section II we review related work on the efficacy of value-based approaches with respect to the economic and managerial implications. A brief overview of computer security assurance and its inherit challenges is provided in Section III. Sections IV and V introduce value-neutral and value-based methods respectively. In Section VI we demonstrate that compliance-based approaches are value-neutral. Section VIII applies the previous findings with a case study of the security firm Armor. This is followed by our final conclusions in Section IX.

II. Related Work

The Literature on the topic of computer security assurance methodologies is extensive. There are a wide variety of competing paradigms, each with several distinct implementations. As the Internet grew into popularity, the first successes were in getting cyber security to be a topic of any relevance at all. Over time this grew into a formalized field of study; complete with a taxonomy of attacks and generalized best practices. This gave way to compliance standards. As governments around the world began enacting security standards, there was a need for risk assessment approaches such as [5], both to inform the content of the standards themselves and to validate that an organization's IT infrastructure was compliant.

Traditionally inspired, value-neutral approaches were explored by the research community. These methods bear large resemblances to general unit testing common in software development circles. Unsurprisingly they suffer from the same issues where all security flaws are considered of equal priority. Given the sheer volume of threats in existence and the dynamic, evolving nature of the threats this type of analysis is inherently noisy and inevitably misallocates precious security assurance resources [1]. There are simply too many vulnerabilities for all to receive equal attention, some form of triage is necessary. As such, risk minimization strategies emerged, but while they do prioritize vulnerabilities, they do so in an ineffective way. Typically, they measure risk terms of risk of exploit rather than economic impact. It has been shown that this strategy for selecting mitigation activities is often inefficient do to the inordinate costs associated with addressing certain risks or because the actual cost to the business of a successful exploitation of the asset is relatively small [4].

In any organization, especially for-profit corporations, every investment must be justified from the standpoint of return. Investments in security assurance are no exception. This presents a challenge for cyber security professionals, who must find a way to calculate and convey the return on the expenditures they seek to get approved. The problem is that, when it comes to capital expenditures in security assurance, the return on investment is that a bad thing does not happen, rather than that a good thing happens [3]. A successful investment prevents some financial, reputational, or information loss from occurring instead of generating revenue. This makes such investments more akin to insurance premiums than more typical capital expenditures that expand capacities or otherwise produce new sources of revenue in the future. From the standpoint of profitability, there is no difference between avoiding a loss and generating income. However, investments that avoid costs are generally less favored. The inability of value-neutral security approaches to measure the return on any investment compounds this problem further, meaning that in essentially all organization's operating under such a paradigm the commitment from upper-level management to security investment is insufficient [2].

To solve these issues, a variety of value-based approaches to computer security assurance have been proposed. Some solutions address the IT infrastructure concerns while others are focused on engineering more secure software. These methods can be incrementally incorporated into an organization's policies by improving the methods for tasks they are already performing such as patch management for COTS [6]. The success of these approaches and the quantifiable metrics they produce can be used to explain and justify expansion into new domains of security assurance

Measuring return on investment is not straightforward in security assurance. Doing so requires degerming the losses that would be sustained had an attempted attack been successful and accurately determine whether a particular investment prevented the breach or if the outcome was simply the result of chance. It is critical that an organization can identify individual investment-outcome pairs if an intelligent analysis is to be performed [3]. Value-based approaches identify security risks and quantify the associated potential losses. The impact of producing quantifiable metrics cannot be overstated. When it is possible to measure risk accurately, the question of the value of loss avoided is answered. With risks identified ahead of time, it is possible to go back through logs and determine if the investment made to mitigate was responsible for. This means that after an attempted breach the ROI can be computed and conveyed to upper-level management. Even if no breach occurs the ROI can still be computed, and the risk profile calculate to show that the expenditure was justified and necessary.

An organization that can compute the return on their investments can do more than just justify the expenditures, they can analyze the computed metrics to inform future decisions. In other words, it allows them to implement continuous improvement into their security assurance programs. Calculating the ROI with respect to each security investment a firm has made allows them to measure its efficacy. If, for

instance, an investment does not produce a positive net return, that informs the firm that they should cease to make the investment, even if no alternative exists to replace it. Investments that do produce net positive return can be compared against one another, and the investments that produce the largest returns can replace those that produce smaller returns.

Continuous improvement can also be applied with intra-investment decisions in addition to inter-investment decisions as discussed previously. Consider an investment into a network monitoring device. The device is reliable and feature rich, meaning that it nets the company a positive ROI. Assume that there are no superior alternatives to the device available on the market. While there is no alternative to the device and its associated expenditures are justified, there is still room for improvement. Different configurations, improved employee training, optimizing related processes, etc. are all potential candidates. Experiments can be run, and the associated ROI's calculated, which can be used to inform business decisions that will improve security outcomes and the return on investment.

Another important consideration for any organization is determining the appropriate level of investment in security assurance. Value-based approaches can provide the necessary data and methods to perform such calculations, unlike their value-neutral counterparts [4]. Remember that security investments are more akin to buying insurance than increasing factory capacity. It would not make sense to purchase car insurance if the premiums were so large that they approached the cost of the vehicle over the lifetime of its use. By the same intuition, and underlying statistical measures that justify it, an organization should only spend some small percentage of the potential loss due to a security breach. Because value-based methods allow a firm to accurately compute risk and costs, they provide the necessary information to determine the overall level of investment an organization should make in computer security assurance.

III. Computer Security Assurance

Computer security assurance is a field of study and domain of work that is concerned with maintaining an effective defense against threat actors seeking to inflict harm and/or gain resources by exploiting computer systems and their networks. The desired outcome is to avoid or minimize the harm to an organization caused by theft (e.g. proprietary intellectual property or financial resources), disrupted business activities, and damage to brand name reputation. While the topic is complex, it can be surmised at a high level by considering the three major components of security.

Before introducing them, it's helpful to first consider the different states that data can exist in, because these states are relevant to goals of some of the major components of security. Data can be at rest, in transit, or in use. Data is defined to be at rest when it is held unused in storage, available to be used at some future point in time if the system requires it. Unopened files on a hard drive are an example of data at rest. We define data as in transit when it is actively being transferred from one location to another. Most of the time we are concerned with

network communication, but data in transit isn't limited to this scenario. Inter-process communication methods such as piping and direct memory access are also examples of data in transit. Data traveling along a bus is an example when hardware security is being considered. Finally, there is data in use, which is simply defined as data that is actively being processed. This can include opened files, working memory, and the storage circuity of the central processor.

All three states of data have important security considerations unique to each of them. If there is a lapse in security with respect to any one of these states it in effect nullifies the security employed in the other states. For instance, no amount of security in the storage of data will prevent an eavesdropper from observing it if it is possible to observe in transit. Hence the data is only safe if there are effective security controls in place for both of these data states. With an understanding of data states, we can now consider the three major components of computer security assurance.

The three major components of security are commonly referred to by the acronym CIA or as the CIA Triad. Confidentiality, the first component, is straightforward. It is simply that a system and its data are only accessible to those who are authorized to do so and that they are inaccessible to those who are unauthorized. This applies to people, but it also applies to computers and even individual software processes as well. The next component, integrity, is concerned with the accuracy of data throughout its different states. Integrity guarantees that the data is unmodified and matches exactly the value it was intended to be. This includes accidental modifications, changes due to errors, and intentional corruption introduced by a malicious actor. Digitally signed executables are an example of a security control that protects integrity, both for data at rest and data in transit. Finally, there is availability. Availability is concerned with making sure that a system is running and accessible during the timeframes and through the methods that it is expected to be. This aspect can be less intuitive at first, because it may seem as though it belongs more in reliability or quality assurance rather than as a major pillar of security assurance. Consider though, how a malicious actor could disrupt services intentionally by shutting down a payment processing server. While the server is down, the organization would be unable to process transactions. This means that business, and therefore, revenues, would be disrupted and the organization would suffer financial losses.

There are many components to assuring that the CIA triad is properly accounted for by an organization's security assurance program. First and foremost is event monitoring. Security Incident Management (SIM) tools monitor devices and the network for suspicious opportunity and flags events accordingly. From there analysts determine if the event warrants further action, usually by consulting the relevant log sources. Problems that are genuine will be passed to incident response teams for remediation. If the situation requires it, digital forensics teams will collect evidence to piece together what happened. This type of audit is usually done to determine what changes could prevent such an attack from being carried out again by some future adversary. Other more proactive measures include threat feed monitoring, penetration testing, vulnerability scanning, and patch management/inventory management.

There are a multitude of technical and market condition problems for security assurance programs. On the technical side, infrastructure has ballooned into large, complex environments to meet the needs of the organizations. Tools have yet to become advanced enough to assist with certain tasks while adversaries work together to produce excellent offensive tooling. Add on the constant change inherit to the IT industry and the technical challenges at hand become self-evident. Finally, there is the human factor. No vault, no matter how advanced it is, is secure if the owner forgets to lock up. Social engineering attacks have shown how even some of the most advanced countermeasures can be circumvented by taking advantage of the human element. How to properly address this issue is a massive area of ongoing research.

Additional challenges are introduced by market conditions. Financial resources are extremely limited, and the complexities of conveying the business case for individual security investments only serves to further aggravate the problem. There is a global shortage of qualified employees across the IT industry. Among specializations, security analysts are among the least numerous. The shortage is comparable to the one in software development.

IV. Value-Neutral Approaches For Computer Security Assurance

As the name implies, value-neutral approaches to security assurance operate without considering the business value of security issues under consideration and, as a result, the process of resolving them. Every potential security issue is considered, with prioritization being done arbitrarily by the security analyst or their supervising manager or without any prioritization whatsoever. Such approaches share a similar resemblance to the early days of unit testing in software development, where tools displayed without consideration of the value of the bug or the potential return of creating a patch that fixes it.

The issues inherit with such approaches quickly became apparent and value-based methodologies emerged to replace them. If this evolution was already experienced by the development community before the rise of computer security assurance programs, why have they not taken these lessons into consideration when designing their programs? The primary issue is that most value-neutral methods of computer security involve quantitative metrics. This means that they are not, strictly speaking, completely value-neutral. However, they measure value in terms of minizine risk of exploit, which often does not align with value in terms of return. Consider the following examples of value-neutral methods that demonstrate this issue.

Methods proposed in [7] are an example of a value-neutral method that shares a close resemblance to older software testing methods. The authors present a tool that checks UML models and c code for compliance with custom security requirements. It even contains useful features for generating portions of secure code from the models directly, which reduces the likelihood of a vulnerability being introduced in the first place. Their methodology contains no way of ranking vulnerabilities, it simply itemizes them. Considering that there is no criterion for the vulnerabilities to be relatively ranked against one another, the methodology also cannot consider how vulnerabilities play into the business case and the potential financial risks they pose to an organization.

Later algorithms introduced into the literature can still suffer from the same problems. This is because they are focused solely on identifying vulnerabilities, such as in the case of [8]. Such methods still have a potential place in security assurance, but only as a first stage to feed input into other methods. They are efficient in identifying problems but offer no guidance as to how to efficiently resolve them. Thus, it is important to realize that such methods are only one small piece in what is required to achieve computer security assurance.

Finally, there is the case of approaches that do indeed consider value, but not in a way that is compatible with business needs. [5] considers not just quantitative risk but as the value of the asset associated with the risk. Hence it is not, strictly speaking, value-neutral. The problem is that is utilizes imprecise tables for determining asset value while also failing to consider a variety of different factors that impact the value of the asset. These include reputational factors and opportunity cost. It is an example of a one size fits all solution that will not be suitable for all organizations.

In summary, value-neutral approaches to computer security assurance are ineffective and inefficient. They fail to consider how the function of security fits into the growth strategy of the business as a whole and do not produce quantifiable metrics applicable to that pursuit. Consequently, they promote malinvestment and make it difficult to convey the value of security investment to C-level executives [2]. Limited funding will be made available and no continuous improvement process will be implemented to maximize the value of the limited resources provided.

V. Value-Based Approaches for Computer Security Assurance

Value-based approaches for computer security assurance consider the real value of vulnerabilities (in terms of potential losses) and investments (in terms of return) in a manner that is consistent with the business outcomes of the organization. As in the case of many value-neutral methods, they begin by identifying vulnerabilities and quantifying the risk that they pose. The difference lies in transforming risk values so that

they reflect the expected losses to the organization should the related vulnerabilities be successfully exploited in an attack.

These calculations can be used to determine what the return on any investment should be. While better informing investment decisions alone makes them vastly superior to value-neutral methods, the potential applications are much greater than just that. These measurements enable a firm to analyze the return on prior investments at an individual level. Investments that fail to generate return can be stopped and successful ones can be compared to select the best one.

Value-based approaches are flexible, and a number of different implementations exist to accommodate different needs and different applications. For instance, the methods detailed in [6] focus on evaluating the security of commercial off the shelf software programs and the ROI of patching and monitoring such systems. A number of value-based methods for security concerns in the actual development of software exist as well. Once such case can be found in [9]. The primary focus of the literature is on organization wide computer security assurance [10], [11], [12], [13].

By transforming risk values in such a way that they account for the expected losses of a security breach should it occur, value-based approaches allow investment decisions to be made using the same statistical analysis an organization would make when considering any insurance purchase. Organization's also gain the opportunity to implement systematic continuous improvement into their computer security assurance approach. Ongoing investments can be canceled or justified based on analysis results. Comparisons can be done to select superior alternatives. The implementation of any particular investment can be optimized by performing the same type of analysis on the subfactors that make it up. Value-based methods are extremely flexible because they rely on outcome driven processes and produce transparent, comprehensible outputs.

VI. Compliant Is Not the Same As Secure

Compliance strategies minimize risk in a value neutral way. The primary focus is to minimize the surface area for an attack, with little to no regard given to the cost benefit ratio of the particular security practice with regard to the specific asset it is being applied to or the specific considerations of the individual organization. Limited resources available for computer security assurance are often squandered through misuse and ineffective allocation.

Some compliance standards are more general, but the vast majority of them are application specific. For instance, HIPPA is a regulatory requirement for organizations handling medical records and PCI is a standard an organization must follow if it wishes to do business with major credit card processors. HITRUST is an example of a security compliance standard that is more general in its application. Some are maintained by independent standards bodies while others are maintained by government agencies.

Many organizations choose to meet their regulatory compliance requirements and consider that to be equivalent to being secure. The problem with this thinking is that compliance standards are created to be useful and implementable to a general audience of organizations. They are not optimized and are not aiming to introduce total security. Instead, they produce guidelines to give an organization a good starting place and to reduce the chances of some of the most basic attacks from succeeding. By nature of being a standard, it will suffer from biased, competing interests and be slow to react. In the highly dynamic world of security the turnover between drafting, ratifying, and implementing standards revisions is too great to be a complete solution.

Having established that compliance-based solutions produce suboptimal security outcomes, let us consider the economic efficiency of them. Compliance-based solutions are value-neutral, at least in the sense that they do not take the organization's bottom line into account. There is some concern insofar as that the standard attempts not to be too burdensome, so some level of efficiency exists, and that they aim to address common security problems, meaning there will be at least some level of efficacy. These assumptions, however, assume that the organization isn't already meeting these obligations some other way and that the threats apply to the induvial organization according to industry averages. Even if the organization is fairly typical in the factors considered by the standard, items outside those factors will not be considered despite being relevant details. Finally, aim to be not bad with respect to efficiency, which is not the same as aiming to be good (i.e. optimal).

We propose that compliance-based approaches for computer security are examples of value-neutral approaches. They can be demonstrated to suffer from the same negative outcomes by showing the overlap in their methodologies and by examining them independently. Both methods of analysis produce consist results. Compliant is not synonymous with secure and compliance-based approaches will under perform in both security outcomes and economic efficiency.

VII. Armor Case Study

Armor Defense Inc. was founded in 2009 as Firehost by retired US army paratrooper Chris Drake. Inspired by valuable lessons gleaned from an extensive litigation process resulting from security issues in a prior endeavor, Drake aimed to solve the clear inadequacies of security tools and practices in the hosting market. Initially they started off as a bolt-on security suite for traditional hosting packages. As the company grew it made a name for itself by becoming the first "Compliance-As-A-Service" solution in the industry. This allowed companies to outsource expensive compliance issues and achieve better security outcomes and ROI than they would on their own. Despite these improvements, Armor was aware of the shortcomings of such an approach to security insurance and began investing in research and development to improve further.

Once the transition from a compliance-based approach to a value-based approach was completed (and to account for shifts in business development strategy that happened during the process) the company rebranded as Armor in 2015, launching the industry's first "Security-As-A-Service" Solution for the public cloud. They have continued to show strong growth figures, have high investor confidence, and are among the fastest growing private companies in the country. As of late

2017 they have grown to over 200 employees and recently completed an $86 million round of venture capital fundraising. Their methods have been tested on a diverse group of hundreds of customers protecting $200+ billion in transactions annually across thousands of machines in public, private, and private clouds [14].

Armor's strategy focuses primarily on getting the greatest possible return in security outcomes for each dollar spent. This makes them an extremely efficient company that can offer excellent security outcomes at a cost far lower than what businesses can typically hope to achieve on their own even when Armor's profit is accounted for.

Most value is derived from minimizing attack surface and disrupting threats early. These methods are cheap and automation friendly, so they have deployed a combination of COTS software and proprietary software to leverage the opportunity. Minimizing the attack surface requires initial configuration, but no subsequent work is necessary. By disrupting threats in early stages of the security kill chain, Armor avoids the complex and expensive task of responding to late stage attacks. The value of expected losses mitigated these tools is not relevant to the calculation because there is immense overlap between them. A firewall, for instance, inhibits a large number of attacks from being conducted at very low cost. Some of these attacks are high value, so return is positive. The lower level threats are mitigated for free as a consequence of addressing the higher-level ones. Thus, the return will always be positive. Continuous improved is achieved by analyzing what makes it through the barriers and proposing changes to prevent the attack from recurring with an improvement to automated systems. Value must be considered at that level, but it is not necessary here.

Threats that make it through the highly optimized, general defenses described about are resolved with great consideration to value. Several tiers of analysts of increasing analyst skill and cost work to triage the problems. Triaging ranks tasks by what level analyst should address them, and what priority among such tasks it is. Some of this is automated and an entry level analyst trained in ranking makes the final determination. The level of analyst used addresses the concern of spending as little as possible resolving an event and the event queue at each analyst level considers the value of threat in terms of expected financial losses to the client. At any point these two criteria have been optimized.

A rigorous continuous improvement process identifies and solves issue in triaging. Analytics reviews consider if the activity was ranked appropriately and if too many resources where spent addressing the problem. Shortcomings are discussed by the team and process changes are considered. If patterns emerge showing that some task is a candidate for automation, it becomes a feature request for the development team or an analyst develops a standalone tool depending on the type of improvement being made.

Armor makes for an excellent case study because they have implemented compliance-based and value-based methods at the highest performance levels in industry. There transition and the growth that follows demonstrates the success of such a shift. Since they have been industry leaders with both approaches, there is not concern that implementation quality is serving as a confounding variable. Armor successfully blocks 99.999% of attacks. They have an average dwell time of less than 1 day, compared to the industry average of 125 days. An independent study by the consulting firm Forrestor on the total economic impact of utilizing Armor's services found that doing business with them would need an ROI of up to 286% over typical industry (i.e. compliance-based) solutions [15]. Armor clearly demonstrates the efficacy and cost savings of utilizing value-based approaches for computer security assurance.

VIII. Conclusions

In this paper, we establish that Value-based methods for computer security assurance produce superior security outcomes at a lower cost than those that are value-neutral. Value-based methods are able to take the specific needs of an organization into account and adjust in response to those needs. They produce quantifiable metrics that can guide investment decisions and justify the business case of security investments. The decisions arrived to are easy to convey to C-level executives, which increases the probability that sufficient levels of funding will be provided.

Additionally, these methods provide the unique opportunity for investments to be analyzed after they are made. The return can be calculated and compared against what was expected. When they don't align, changes can be made to resolve the issue. If some investments pan out better than others, the organization can replace them. Even if no superior replacement is found, the same techniques can be applied to the individual aspects of the security solution to implement continuous improvement within it and maximize the output it produces.

We contribute a novel analysis of compliance-based approaches and demonstrate that they are in fact value-neutral. Because they do not consider the specific needs of the organization, they suffer from the same problems. Switching from compliance-based to value-based methods comes at no additional long-term cost and provides the majority of compliance for free. What remains can be dealt with as would be under a compliance-based approach. Such items are dealt with at equal cost, not greater, meaning that there are no losses

incurred by switching approaches. Our case study of the security firm Armor demonstrates the veracity of our claims in the real world. It shows that security outcomes can be improved by over an order of magnitude and that switching to value-based methods can yield a return of up to 286%.

REFERENCES

[1] Gunnar Peterson. “The economics of finding and fixing vulnerabilities in distributed systems”, Proceedings of the 4th ACM workshop on Quality of protection (QoP '08). ACM, New York, NY, USA, 2008, 1-2.

[2] Kunwoo Kim and Jungduk Kim. “A Role of Information Security Committee based on Competing Values Framework”, Proceedings of the 17th International Conference on Electronic Commerce 2015 (ICEC '15). ACM, New York, NY, USA, 2015, Article 32.

[3] Nishtha Kesswani and Sanjay Kumar. “Maintaining Cyber Security: Implications, Cost and Returns”, Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research (SIGMIS-CPR '15). ACM, New York, NY, USA, 2015, 161-164.

[4] Lawrence A. Gordon and Martin P. Loeb. “The economics of information security investment”. ACM Trans. Inf. Syst. Secur. 5, 4 (November 2002), 438-457.

[5] M. U. Aksu et al., "A quantitative CVSS-based cyber security risk assessment methodology for IT systems," 2017 International Carnahan Conference on Security Technology (ICCST), Madrid, 2017, pp. 1-8.

[6] Y. Chen, B. Boehm and L. Sheppard, "Value Driven Security Threat Modeling Based on Attack Path Analysis," System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on, Waikoloa, HI, 2007, pp. 280a-280a. doi: 10.1109/HICSS.2007.601

[7] Jan Jürjens and Jorge Fox. “Tools for model-based security engineering”, Proceedings of the 28th international conference on Software engineering (ICSE '06). ACM, New York, NY, USA, 2006, 819-822.

[8] J. Bozic, B. Garn, D. E. Simos and F. Wotawa, "Evaluation of the IPO-Family algorithms for test case generation in web security testing," 2015 IEEE Eighth International Conference on Software Testing, Verification and Validation Workshops (ICSTW), Graz, 2015, pp. 1-10.

[9] Thomas Neubauer, Markus Klemen, and Stefan Biffl. “Business process-based valuation of IT-security”, Proceedings of the seventh international workshop on Economics-driven software engineering research (EDSER '05), Kevin Sullivan (Ed.). ACM, New York, NY, USA, 2005, 1-5

[10] S. A. Butler, "Security attribute evaluation method: a cost-benefit approach," Proceedings of the 24th International Conference on Software Engineering. ICSE 2002, Orlando, FL, USA, 2002, pp. 232-240.

[11] Anis Ben Aissa, Robert K. Abercrombie, Frederick T. Sheldon, and Ali Mili. “Defining and computing a value based cyber-security measure”, Proceedings of the Second Kuwait Conference on e-Services and e-Systems (KCESS '11). ACM, New York, NY, USA, 2011, Article 5.

[12] L. B. Othmane and A. Ali, "Towards Effective Security Assurance for Incremental Software Development the Case of Zen Cart Application," 2016 11th International Conference on Availability, Reliability and Security (ARES), 2016, pp. 564-571.

[13] A. Belalcázar and M. Ron and J. Díaz and L. Molinari, "Towards a Strategic Resilience of Applications through the NIST Cybersecurity Framework and the Strategic Alignment Model (SAM)," 2017 International Conference on Information Systems and Computer Science (INCISCOS), 2017, pp. 181-187.

[14] https://www.armor.com/history/

[15] Bob Cormier. “The Total Economic Impact of Armor solutions” Forrestor Research Inc. 2017, pp. 1-21.