Applied Computing and Informatics (2015) **11**, 144–157

Saudi Computer Society, King Saud University

Applied Computing and Informatics

(http://computer.org.sa)
www.ksu.edu.sa
www.sciencedirect.com

ORIGINAL ARTICLE

Clear and present danger: Interventive and retaliatory approaches to cyber threats

Danilo V. Bernardo *

Db2P Research Institute, Bathurst Street, Sydney, NSW 2000, Australia

Received 3 May 2014; revised 14 September 2014; accepted 23 November 2014
Available online 4 December 2014

KEYWORDS

Cybersecurity;
Cyber warfare;
Cyberattacks;
Interventive;
Retaliatory;
Intelligence sharing

Abstract Organizations, including governments, have been attempting to address cyber threats for years by deploying technologies (e.g., security perimeter defences). These technologies are overarching policies and regulations designed to encourage resilient cybersecurity strategies that safeguard not only data, but also properties and human lives. Implementing these technologies is one thing, but ensuring their effectiveness is another. Lack of effectiveness and inability to satisfy existing government requirements and approaches in dealing with cyber threats and attacks are likely to continue until better approaches are employed. These approaches may emanate from effective regulations, intelligence gathering and sharing, and good security practices to workable alliances and interactions with other communities. This work is proposing approaches based on the premise that cybersecurity strategies must adhere to and be guided by the effectiveness criteria: that is, intervention and retaliatory approaches should be employed and utilized on the basis of their empirically demonstrated effectiveness to combat cyber threats.

* Tel.: +61 475 195 839.
E-mail address: bernardan@gmail.com.
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.aci.2014.11.002

1. Introduction

In achieving effective cybersecurity (http://belfercenter.ksg.harvard.edu/events/6230/intelligence_in_the_private_sector.html, 2014), as in employing effective cyber warfare preparation and governance, the importance of quickly recognizing cyber threats concerns the most basic elements of their identification, recognition, and employment of appropriate courses of action.

It is a challenge for policy makers and practitioners to effectively determine potential threats as early as possible. Hence, when cyber strategies (http://belfercenter.ksg.harvard.edu/events/6230/intelligence_in_the_private_sector.html, 2014; Bernardo and Chua, 2013) are examined, there is an ideal opportunity to observe the means through which organizations, governments in particular, become challenged in adjusting to the expectations of their stakeholders under the conditions of alliances, cooperativeness, socio-demographic values, and other practical influences.

In these conditions, the opportunity must be explored to develop processes and approaches that are survivable long-term. These conditions, however, do not reflect effective governance and, most of all, effective strategies in dealing with cyber threats, because these conditions are: firstly, influenced by practitioners' lack of effective interventive approach that falls short of compliance with the regulations and exercise of better security mechanisms; and secondly, found to be lacking comprehensive and effective retaliatory approach to launch mitigation strategies (e.g., counterattacks, etc.).

Attaining viable strategies to address cyber threats and attacks remains a challenge (http://belfercenter.ksg.harvard.edu/events/6230/intelligence_in_the_private_sector.html, 2014; Bernardo and Chua, 2013) due to lack of concentration on tailoring approaches to address appropriate actions to cyber threats: (a) key but uninformed practitioners are too conservative in meeting their agenda to carry out their own strategies on dealing with cyber threats; (b) another is the slowness of legitimate governments to move beyond mere identification of cyber threats by introducing enforceable regulation and actions, and viable solutions to curb and address them, and to fully recognize the importance of alliances with industries and other governments to have unified and effective approaches to combat cyber threats.

Central to the process of this phenomenon is the general perception that trivializes cyber threats and cyber security practices and the kind of impact that led to the lack of effective approaches. Consequently, practitioners become more reluctant to stably carry out their responsibilities and raise their level of awareness in order to minimize threats.

Theory and research into cyber security should therefore shift across various perspectives, and not be limited to: (1) retaliatory and interventive approaches, (2) compliance to existing regulations, (3) multi-way process and contemporary view of cybersecurity as fundamentally an emergent necessity of interaction and

alliances in which governments and industries jointly develop stronger cyber-policing and intelligence-sharing capabilities, and (4) appropriate statistical methods to achieve effective threat detection and sustainable solutions.

Interventive approach is introduced, addressing, in particular, the underlying practitioners' low level of awareness and their limited intelligence sharing, in terms of capabilities and access, and knowledge in dealing with cyber threats on a large scale, and implementing specific courses of action in given circumstances (during the onset of confirmed cyber attacks).

Methods for developing retaliatory approach, on the other hand, is reviewed and investigated. These include ways to detect and subsequently derail the source of the cyber attacks, and to execute defence mechanisms that can lead to infrastructure shutdown to halt further attacks and minimize damage to properties. These mechanisms can include terminating communication services across regional domains (e.g., DNS-domain name services) that provide the means to channel collaborative cyber attacks.

This work captures the importance of effective cybersecurity strategies from the standpoint of statistical representations (Berger and Wolpert, 1988) to symbolic interactionism (Blumer, 1969; Bernardo and Smith, 1994), which represents a shifting relationship between practitioners and governments attempting to fit their lines of agenda together to develop effective and interactive cybersecurity strategies.

This paper is organized as follows: Sections 2 provide an overview of criteria and methods, Sections 3 and 4 highlight discussions, and Section 4 concludes this work.

2. Guide to developing cybersecurity approaches

Competing requirements (e.g., regulations, technology, intelligence, goals, etc.) produced effectively advance, control-capable approaches, which can be used to guide practitioners.

These approaches form strategies on cybersecurity that can assist and enable practitioners to select and employ consistent determination relevant to their infrastructure, and which have been found to be effective for the desired outcome (Bernardo et al., 2009; Bernardo and Chua, 2013). These approaches should contain components that refer to the requirements that can be systematically varied within the intervention process, and which are capable of reliable deployment across organizations. To meet these requirements, concepts and variables must be clearly identified, defined, and linked to empirical referents.

Statements of interventive and actions of retaliatory approaches must contain explicit predictions of the relationship between the inputs (processes), tactical courses of action and the desired outcomes (e.g., minimization of threats and validations of enforced mechanisms, and introduction of strike back mechanisms).

Interventive statements and actions of retaliation of this nature serve three indispensable functions: (1) they facilitate and deliberate selection of intelligence

work by practitioners of a given approach from a number of possible alternatives on the basis of its applicability to a particular situation and infrastructure; (2) they provide the framework within which their empirical validity can be tested – that is, they enable practitioners to design cybersecurity architectures and infrastructures in which the effectiveness of both interventive and retaliatory assumptions can be rigorously investigated and validated; and (3) they facilitate tactical countermeasures and counterattacks, whenever possible, to halt any efforts of derailment and curtailment of services solely dependent on cyber-technology.

These criteria must be met if the creation of both approaches is to contribute meaningfully to knowledge capable of guiding practice in cybersecurity. Of these criteria, two basic ones will be used for classifying both approaches: (1) whether the interventions and retaliation – the independent variables or components – are empirically denotable and can be reliably enacted by practitioners and, therefore, replicated in the subsequent review and in practice and (2) the extent to which the outcomes against which the effectiveness of interventions and counter-attacks is assessed are measured with sufficient validation to allow reliable replication to other organizations across the geographical locations.

2.1. Expected outcome

The utility of differentiating the outcomes of the defined interventive and retaliatory approaches depends on the specific goal set in a particular effort to address cyber threats. The attainment of maximum outcomes (MO) denotes the extent to which the effort is successful and determines the organization's readiness to combat cyber threats, whereas intermediate outcomes (IO) are those deemed to be necessary preconditions of the maximum outcomes.

This work relies on the efficacy of interventions and retaliations that legitimately targets either intermediate or maximum outcomes. However, the evaluation effort concerns the extent to which problems are addressed successfully through interventive and retaliatory approaches; therefore maximum outcomes must be included as dependent variables.

The central focus in this work is concerned where existing efforts appropriately address the different needs for effective practice, and the analysis in this work is guided by the goal set in the preceding sections. Existing works and practices particularly in major industries (e.g., telecommunications, transportation and electricity), though limited, have been analyzed to assess the relative emphasis on cyber security research, which can contribute to the community of practice on the effectiveness of both approaches and the relationship between replicability of these approaches. With some countries or organizations lacking cybersecurity preparedness and guidelines, this work focuses on available roadmaps and collected data sets available, instead of government-restricted classified information.

2.2. Sampling

It is important to select industries (e.g., academe, governments, and private financial sectors) and provide an assessment period to reasonably represent the primary current thrusts of cybersecurity research. The practices are focused on organizations across the US, UK, Asia Pacific (especially on those recently targeted by cyber attacks, such as Philippines, South Korea, Vietnam, the US, and Australia). This work builds on initially collected data from 3 identified organizations (Bernardo, 2012, 2013; Bernardo and Chua, 2013) with regional presence in the UK, US and Asia, and focuses on one recently completed survey on risks and threats on cloud computing. The choice of the work specifically on cloud computing in this sample can be considered more opportunistic rather than monolithic. Given the recent popularity of cloud computing across governments and industries and due its identified risks, the choice has been alluded to the benefits of understanding the current trends and of further underscoring the importance of cyber threats across many infrastructures.

To observe a situation where cyber threats are suspected to be taking place, it is important to define that central to the interaction where these occur is the significant process of identifying and differentiating cyber attacks from the other attacks (i.e., localized) that occur on a certain period; considering the impact of these attacks into account; and responding by acting according to the existing courses of action.

The outcome of this observation influences the development of cybersecurity approaches. However, this observation should be supported by statistical representations to provide empirical evidence. These further solicit and substantiate the development of approaches that require resources.

2.3. Statistical representations

There has been a continuing thrust to identify and quantify attacks, which considered incidents to determine appropriate mitigation strategies to obfuscate them. Organizations developed and improved their courses of action, including identification and frequencies of incidents to determine if they are localized or if these are considered large-scale cyber attacks. These plans include statistical representations, which are tailored to the organizations and practitioners of attacks, as discussed in 3.1.1 (Bernardo, 2012, 2013; Bernardo et al., 2009; Bernardo and Chua, 2013).

2.3.1. Ranking method

$$di = \sum_{j=1}^{m} |rij - cj| (i = 1, \ldots, n). \tag{1}$$

where n = individuals/organizations and m = risk areas. Let rij be the rank of the ith organization on the jth risk ($i = 1,...n$ and $j = 1,...m$) (Bernardo, 2013; Bernardo et al., 2009).

If cj is the group rank for the jth risk, then the ith organization's absolute distance from the group ranking.

Data collected in the following works (Bernardo, 2012, 2013; Bernardo and Chua, 2013) were also relevant to supply components for representation in Eq. (1). Results from Bernardo (2012, 2013) are found on Table 1.

Additionally, we look at the works (Bernardo, 2012, 2013; Bernardo and Chua, 2013; Bernardo and Hoang, 2012; Bernardo and Smith, 1994) surveyed across organizations in different industries using basic frequency analysis and correlation method (FC).

2.3.2. Frequency and correlation method (FC)

- $f(i)$ frequency of incidents i in given space.
- φ (a) correlation of frequency of incidents identified assuming specific number of attacks is a (*is a numerical representation of attacks*).

$$-\varphi(a) = \Sigma 0 \leqslant i \leqslant \mathrm{n} f(i) p(i-a) \tag{2}$$

$P(x)$ is frequency of incidents identified across a given period t as example we selected one organization adopting cloud computing.

The data (Table 1) are gathered through a case survey conducted (http://belfercenter.ksg.harvard.edu/events/6230/intelligence_in_the_private_sector.html, 2014). Full results of this particular work are found on Appendix.

The ranking of each threat is gathered from the result of the survey conducted with organizations with 35,000 clients based in Melbourne, Australia, Hong Kong, and Malaysia (Bernardo, 2012, 2013; Bernardo et al., 2009; Bernardo and Chua, 2013).

From Eq. (1), the ranking is organized from survey returned.

Thereof,

Sequence = CR1CR2CR4CR6

Table 1 Common threats of cloud computing.

CR1	1	Uncoordinated change controls and misconfigurations	.095
CR2	2	Inadequate Access Control Management	.090
CR3	3	Single point of failure/coding	.082
CR4	4	Single tier security	.080
CR5	5	Poor IP pool management	.073
CR6	6	Loose data distribution	.070
CR7	7	Cross tenancy workloads	.065
CR8	8	Unmonitored/unassigned resources	.058
CR9	9	Lack of configuration information and uniformity	.052
CR10	10	Inherent risks of cloud computing	.045
CR11	11	Environmental/calamities	.033

Number of attacks = 3

Frequency of each threat is found on Table 1 and summarized in Fig. 1.

Note that CR1 ranks the highest as shown in the figure, with CR 11 ranking the lowest.

From Eq. (2) so here,

$$\varphi(a) = 0.095p(1-a) + 0.090p(2-a) + 0.082p(3-a) + 0.080p(4-a) + 0.073p(5-a) + 0.070p(6-a) + 0.065p(7-a) + 0.058p(8-a) + 0.052p(9-a) + 0.045p(10-a) + 0.033p(11-a)$$

Most plausible sequence based on φ

- $a = 2$, $\varphi(a) = .0410$
- $a = 3$, $\varphi(a) = .0575$ CR1CR2CR4CR6
- $a = 4$, $\varphi(a) = .0252$
- $a = 5$, $\varphi(a) = .0190$

The threat value is 3 which is CR4 (Single Tier Security).

We arrived to CR4 since we set an initial value of 0 when determining φ.

The result highlights that threat is localized albeit the accuracy of this description is depending on the frequencies and threat's criticality. Criticality is defined by Bernardo (2012) and Bernardo and Chua (2013).

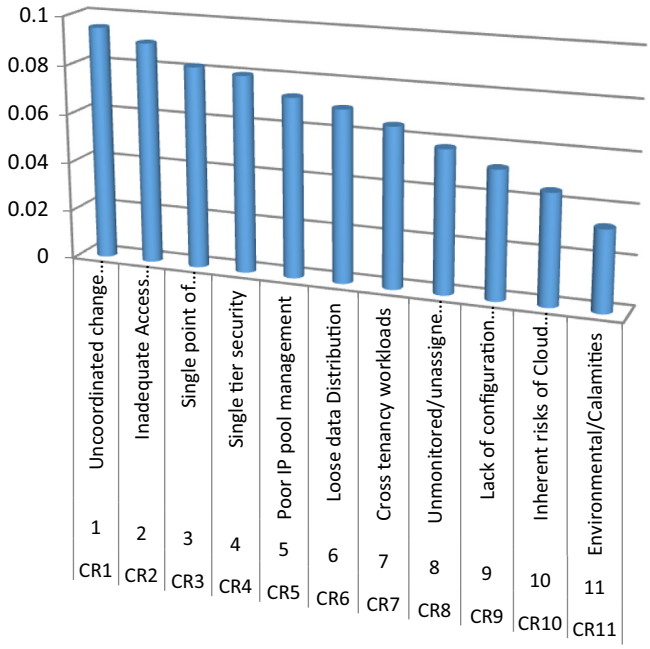

Figure 1 Ranking and Correlation.

$$Criticality = cost * Freq\ of\ Threat\ s + cost * mitigation \tag{3}$$

Eq. (3) represents the cost involved when a threat arises and the costs to mitigate it. This therefore does not necessarily means that the higher the frequency of a threat occurring, the least likely it is localized.

Threats are considered large scale when they have high frequencies and with high costs, that is – the criticality and impact are considered high by practitioners.

2.3.3. Practical application: Stochastic matrix and Markov process (Brooks, 1998)

The next method is validating threats. Given that the first state validation of a suspected threat, (Bernardo and Chua 2013; Bernardo, 2012).

I	(TCP/IP Threats validation)	30%
II	(Application threats validation)	20%
III	(Others/Users/Environmental threats validation)	50%

We need to determine the rate of the second, third, and fourth validations, assuming that the transition probabilities for the given intervals are presented by the matrix

$$\begin{array}{cccc} & \text{To I} & \text{To II} & \text{To III} \\ \boldsymbol{A} = & 0.8 & 0.1 & 0.1 \quad \text{From I} \\ & 0.1 & 0.7 & 0.2 \quad \text{From II} \\ & 0.0 & 0.1 & 0.9 \quad \text{From III} \end{array}$$

Remark. A square matrix with nonnegative entries and row sums all equal to 1 is called stochastic matrix. $\boldsymbol{A}$ therefore is a stochastic matrix. A stochastic process (Berger, 2006; Brooks, 1998) for which the probability of entering a certain state depends only on the last state occupied (and on the matrix governing the process) is called a Markov process (Bernardo and Chua, 2013; Bernardo and Smith, 1994). Note: Markov Process is a prerequisite example in understanding how the approach can be beneficial in identifying threats and generating courses of action.

Solution. From matrix $\boldsymbol{A}$ and the first state we can compute the second state:

I (Network related threat validation) $0.8 * 30 + 0.1 * 20 + 0.50 = 26$ [%]
II (Localized threat validation) $0.1 * 30 + 0.7 * 20 + 0.1 * 50 = 22$ [%]
III (Other threat validation) $0.1 * 30 + 0.2 * 20 + 0.9 * 50 = 52$ [%].

The sum is 100%, as it should be. We present this in matrix form. Let the column vector x denote the first stat. Thus,

$\mathbf{x}^{\mathbf{T}} = [30\ 20\ 50]$. Let $\mathbf{y}$ denote the second state.
Then

$$\mathbf{y}^{\mathbf{T}} = \mathbf{x}^{\mathbf{T}}\boldsymbol{A} = [30 \quad 20 \quad 50] \begin{matrix} 0.8 & 0.1 & 0.1 \\ 0.1 & 0.7 & 0.2 \\ 0 & 0.1 & 0.9 \end{matrix} = [26 \quad 22 \quad 52]$$

Similarly, for the third and fourth we get the state vectors, as you may verify,

$$\mathbf{z}^{\mathbf{T}} = \mathbf{y}^{\mathbf{T}}\boldsymbol{A} = (\mathbf{x}^{\mathbf{T}}\boldsymbol{A})\boldsymbol{A} = \mathbf{x}^{\mathbf{T}}\boldsymbol{A}^2 = [23.0 \quad 23.2 \quad 53.8]$$
$$\mathbf{u}^{\mathbf{T}} = \mathbf{z}^{\mathbf{T}}\boldsymbol{A} = (\mathbf{x}^{\mathbf{T}}\boldsymbol{A}^2)\boldsymbol{A} = \mathbf{x}^{\mathbf{T}}\boldsymbol{A}^3 = [20.72 \quad 23.92 \quad 55.36].$$

In the second state, the network related threat validation will be 26%, the localized threat validation is 22% and the other threat validation 52%. For the third state the corresponding figures are 23%, 23.2%, and 53.8%. For the fourth state, they are 20.72%, 23.92% and 55.36%.

The above example can assist in achieving reasonable estimations for how validations should be performed in future threat identification using basic Markov process. The inputs (Brooks, 1998; Chen et al., 2007; Congdon, 2003; Goldstein, 2006; O'Hagan and Forster, 2004) and assumptions to be accurate, they must be based on data collected on field.

2.4. Summary

The methods highlight essential approaches in determining ways to effectively identify and address cyber attacks. This means that from the point of view of theory, practice, and method, cyber attacks may be observed and validated through direct observation; one may also experience it, comparing by gauging the existing criteria, using the techniques and methods presented, and benchmarking them against the others as the attacks continue to unfold over time.

The initial observation of the recent cases is the discovery of lack of effective strategies, technologies, and resources to carry out effective cybersecurity. This observation is made as a result of static, one-way observation on incidents that reportedly occurred. One-way observation means observing circumstances with limited interaction (e.g., lack of active data gathering, of active participation of those involved, and of consistent monitoring and review, to name a few). Dealing with reports of cyber attacks must therefore involve a dynamic multi-way complex process of interactions and intelligence sharing between those who are tasked to take courses of action and those who are directly affected by them and those who defined governance and compliance (e.g., emergency response group, government funded groups, and industry).

It is not uncommon to view such interactions as interpretation of reality of effective collaboration through strong alliances. These interactions and interpretations, however, can break down at any stage throughout the process. Therefore, it

is important that unified approaches (e.g., a combination of approaches on Table 4) are developed through acceptable methods.

Statistical representations certainly provide ways to define and determine important inputs for the use of methods and processes in determining threat profiles for practitioners. These are important to collectively introduce sustainable approaches to deal with cyber threats.

Low awareness of cyber threats and lack of satisfiable and unified approaches to address them stem from lack of collaboration, compliance to regulations, and, most importantly, methods to developing common strategies.

3. Discussion and framework

Trends in the development of conceptual framework to detect cyber threats have paralleled those in specific regions (Bernardo et al., 2009; Bernardo and Smith, 1994) where threats have occurred and/or are continuing. In recent years, the problem of cyber threats has become an identifiable issue for many organizations that can be addressed by the appropriate intervention.

The problem of cyber threats can be drawn from a cultural or anthropological reason, or just merely lack of political will to invest resources to develop effective intervention strategies.

This work proposes conflict-enculturation (awareness and adaptation of environment susceptible to attacks) as a model of tackling cyber threats through alliances, intelligence sharing, participation and interaction. The major thrust of this approach has been the deep concern for the analysis of meaning, in which governments consider the use of cyber warfare and community involvement to advance cybersecurity and adapt to the demands of peoples' dependency on the Internet.

It is therefore important to raise fundamental questions, such as: (1) Have social and cultural behaviors of both governments and industries toward cyber threats played an important role in defining interventive and retaliatory approaches to address cyber threats? (2) What approaches specific to governments are required to tackle these threats? (3) How do governments and industries achieve outcomes that meet their respective cybersecurity agenda?

These questions are best conducted in longitudinal studies across industries. A periodic analysis of trends may assist in creating methods that raise awareness and address concerns on how cyber threats can be quickly identified, validated, and resolved. Nonetheless, securing cyber-infrastructure remains a challenge to many, especially in an era of cyber threats.

To introduce a brief review of the substance underlying the perspectives on cyber threats, Table 3 highlights a partial framework of the ingredients for determining cyber threats. There are similarities between each approach, illustrating their efficacy.

As presented earlier in Section 2, the approaches on Table 2 highlight the attainment of maximum outcomes (MO), which denotes the extent to which the effort is

Table 2 Values of φ.

A	φ (a)	A	φ (a)	A	(a)	A	φ (a)
0	.0482	3	.0575	6	.0660	9	.0267
1	.0364	4	.0252	7	.0442	10	.0635
2	.0410	5	.0190	8	.0202	11	.0262

Table 3 High level framework.

Cyber threats – more of social and political and less of a technical failure	Interaction/participation and cyber threats analysis multi-way process
Cyber threats motivate initial perspectives which are culturally adaptive Induced propensities, attitude and values toward regulations and differing demographical and cultural perspectives Interact with various contexts with disregard for exercising sensitivity and respect	Relationship between governments extended to group dynamics Community functions as joint agents influencing individual response in the context of cyber threats Strategies constructed through interaction among participants to channel and exchange viewpoints to raise awareness of existing cyber threats

Table 4 General approaches.

Approaches	Outcomes	Maximum/ intermediate
Alliances, collaboration	Practice based participation	IO
Interventive approach	Practice based approach, tailored solution, security architecture	MO
Cyber security community of practice	Specific requirements of cyber big data a security	MO
Integration of government regulations on cyber security strategies into industries (particularly those in public utilities, e.g., transportation, electricity, water and communications to name a few)	Establishment of community of practice related to focusing on cyber threats. Collaborated efforts addressing issues with practical solutions and long term outcomes	MO/IO

successful and determines the organization's readiness to combat cyber threats, whereas intermediate outcomes (IO) are those deemed to be necessary preconditions of the maximum outcomes.

Surveys and studies focusing on the efficacy of interventive and retaliatory approaches may legitimately target either intermediate or maximum outcomes.

To consider the proposed approaches, it is best to frame a practical architecture, as part of the overall goal of achieving maximum outcomes (MO).

As a guide, Tables 5 and 6 highlight the critical components defined in this work for the creation of a security strategy. The components include, but are not limited to, the selected methods discussed in Section 2.

Specific components for retaliatory approach (Table 6) focus on countermeasures and counterattacks where cyber attacks have been mounting – highlighting

Table 5 Specific components under interventive approach.

Stages and components	Determination for security architecture
Validation method (Bernardo, 2012) Type post implementation	Accurately detect anomalies post implementation of systems that support infrastructures
SDL (Bernardo, 2013) Type all cycle	Microsoft's' Security Development Lifecycle (SDL) has set a standard for software and product development. This describes a security requirement definition at the initial phase of the projects, one that involves an analysis of threat modeling at the systems design phase, a static program analysis at the implementation phase, and the penetration test at the test phase (Bernardo, 2013)
Ranking method (Bernardo, 2013; Bernardo et al., 2009; Bernardo and Chua, 2013)/ correlation Type PRE and POST	Prioritizing risks to ensure appropriate mitigations put in place
Other tailored components (Security technology, governance and processes)	Technical architecture focusing on integrating viable security mechanisms and technologies. Governance and Standards

Table 6 Specific components under retaliatory approach.

Stages and components	Determination for the offensive actions
DEFENCES	Strike back capabilities, system tracking and review
ISOLATION	Blocking sources, shutting systems and core infrastructures
SURVEILLANCE	Review attacks and determine courses of actions ie., intervention from agencies, advice from regulators

the need for governments and organizations to form better approaches to control and minimize damage.

The trends of alliances encourage participation and interaction that provide greater access to many experts and tools. Awareness of the issue, of course, can be achieved and raised through tailored approaches. Some organizations, however, have limited opportunities to forge alliances that encourage participation, but engaging with other communities is an important step to developing interaction that can result in feasible approaches.

4. Conclusion

The introduction of satisfiable approaches ensures that there exists an ongoing process encompassing all of the broadly identifiable stages within the defined cybersecurity strategy.

The important element in contemporary cybersecurity, however, is the fact that cyber threats are not solely a technical phenomenon, but also a social one, resulting from an act of behavior that stems from cultural or political action that occurs throughout a cyber attack.

Integrating viable interventive and retaliatory approaches within the cybersecurity strategy through alliances, technology, processes, rules of engagement, intelligence gathering and sharing, statistical methods, participation and interaction with communities of practice (where their use may significantly achieve concomitant economic and political risks that will not derail national security and inflict damage to one's assets) remains an important case for organizations to consider, especially today when cyber threats are prevalent.

The increasingly complex threats to organizations, furthermore, highlight the need to explore the use of intelligence by industries to develop the proposed approaches. According to the recent work (http://belfercenter.ksg.harvard.edu/events/6230/intelligence_in_the_private_sector.html, 2014), governments are unable to share classified information about threats. As a result, practitioners are creating their own intelligence capabilities within their organizations. The work (http://belfercenter.ksg.harvard.edu/events/6230/intelligence_in_the_private_sector.html, 2014), which involved corporate leaders, strongly raises questions about the need of industry intelligence gathering and sharing, such as, ''How do companies organize to obtain it, and how can the government support them?'' ''Is this a growing trend?'' ''How do companies collaborate in intelligence?'' ''How do the governments view private intelligence efforts?'' ''How do private and government intelligence entities relate to one another?'' and ''What does this all mean for the future of intelligence work?''

Future work will be focused on exploring these compelling questions.

Appendix A

Code	Rank	Risks/threats (2011/year)	Likelihood	Impact	Frequencies	Counter measures	Action
CR1	1	Uncoordinated change controls and misconfigurations	Moderate	M	.095	Applicable governance, control and auditing	Avoid
CR2	2	Inadequate Access Control Management	Moderate	M	.090	Role-based access control	Reduce
CR3	3	Single point of failure/coding	Moderate	M	.082	Service downtime	Reduce
CR4	4	Single tier security	Likely	H	.080	Predicate and homomorphic encryptions	Avoid
CR5	5	Poor IP pool management	Moderate	M	.073	Lock step approach in IP assignment and re-assignment	Reduce

(*continued on next page*)

Appendix A (*continued*)

CR6	6	Loose data distribution	Moderate	M	.070	Specific data ownership and storage management	Reduce
CR7	7	Cross tenancy workloads	Moderate	M	.065	Platform attestation, ensuring CSP meets SLA/OLA	Reduce
CR8	8	Unmonitored/ unassigned resources	Likely	H	.058	Applicable governance, control and auditing	Avoid
CR9	9	Lack of configuration information and uniformity	Unlikely	L	.052	Effective dependency map for each resource/tenant	Reduce
CR10	10	Inherent risks of cloud computing	Moderate	M	.045	Virtual private cloud at the premium rate, segregating logical and physical infrastructures	Avoid
CR11	11	Environmental/ calamities	Unlikely	L	.033	Applicable mitigation strategies, and governance , disaster and business continuity programs	Reduce

References

Berger, J.O., 2006. The case for objective Bayesian analysis. Bayesian Anal. 1, 385–402.

Berger, J.O., Wolpert, R.L., 1988. The Likelihood Principle. The Institute of Mathematical Statistics, Haywood, CA.

Bernardo, D.V., 2012. Securing the cloud, dispelling fears: ways to combat climate change 'Network-Based Information Systems (NBiS), 15th International Conference, 26–28 Sept. 2012, pp. 787–793.

Bernardo, D.V., 2013a. Utilizing security risk approach in managing cloud computing services. 15th International Conference Network-Based Information Systems (NBiS), Sept, 2013.

Bernardo, D.V., Chua, B.B., 2013. Random validation and fault detection method in systems implementations. 13th International Conference on Intelligent Systems Design and Applications (ISDA).

Bernardo, D.V., Hoang, D., 2012. Security risk assessment: toward a comprehensive practical risk management. Int. Inf. Comput. Sec. 5 (2), 77–104.

Bernardo, J.M., Smith, A.F.M., 1994. Bayesian Theory. Wiley, New York.

Bernardo, D.V., Chua, D.B., Hoang, D., 2009. Quantitative security risk assessment: An empirical method. IEEE CISIM2009 Proceedings.

Blumer, H., 1969. Symbolic Interactionism: Perspective and Method. Prentice-Hall Inc., NJ.

Brooks, S.P., 1998. Markov Chain Monte Carlo Method and its application. J. R. Stat. Soc. Ser. (The Statisticia) 47 (1), 69–100.

Chen, T.Y., Huang, D., Tse, T.H., Yang, Z., 2007. An innovative approach to tackling the boundary effect in adaptive random testing. In: Proceedings of the 40th Annual Hawaii International Conference on System Sciences, p. 262a.

Congdon, P., 2003. Applied Bayesian Models. Wiley, Chichester, UK.

Goldstein, M., 2006. Subjective Bayesian analysis: principles and practice. Bayesian Anal. 1, 403–420.

http://belfercenter.ksg.harvard.edu/events/6230/intelligence_in_the_private_sector.html (accessed 10.02.14).

O'Hagan, A., Forster, J.J., 2004. Bayesian Inference, 2nd ed., Vol. 2B, Edward Arnold, London.