International Journal of Advance Research in Science and Engineering
Volume No. 13, Issue No. 04, April 2024
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Holistic Cybersecurity Risk Management Framework

Prof Sheetal Laroiya[1], Rashminder Singh[2], Ianur Alam Barbhuiya[3]

[1,2,3]*Department of Computer Science and Engineering*

Chandigarh University Mohali, Punjab, India

sheetal.e15433@cumail.in, rashmindersinghrandhawa@gmail.com

ianuralam12340@gmail.com

Abstract:

The aim of this paper is to present a comprehensive framework for implementing cyber security strategies, termed the Implementation Framework for Holistic Cyber Security (HCS-IF). Drawing from an extensive literature review, the HCS-IF is intended to provide a unified, systematic, and integrated approach to cyber security strategy execution. The framework efficiently meets critical cyber security demands by utilizing high-level conceptual security controls, solutions, and procedures from the domains of information security or cyber security management, software engineering, and project management. Through collective interaction and cooperation of its components and controls, the HCS-IF facilitates the execution of information security strategies efficiently. A comparative analysis with existing frameworks shows the superior performance of the HCS-IF across various evaluation criteria. This study offers valuable insights for governments looking to implement cyber security strategies at a national level and equips practitioners with the necessary tools to tackle implementation challenges comprehensively.

Keywords: *Implementing a holistic framework, managing information security, implementing strategies, strategic controls, and cyber security.*

1. Introduction:

In the context of cybersecurity, protecting national interests in the digital era requires the development and execution of strong cyber security strategies (CSSs). These strategies usually include protocols for developing, implementing, and assessing the strategies. In order to effectively translate strategic objectives into concrete actions,this article focuses exclusively on the strategy implementation phase.

Two main reasons are the driving forces for this research. First and foremost, comprehensive and well-coordinated frameworks are desperately needed in order to successfully implement CSSs atthe federal level. In order to reduce cyber threats and safeguard vital infrastructures, it is necessary to take a more cohesive approach to cybersecurity frameworks, which frequently display fragmentation and differing degrees of efficiency. Implementing security at the national level not only makes early threat identification and risk mitigation easier, but it also gives decision-makersthe ability to react quickly to new threats. In addition, it encourages cooperation between various stakeholders, such as individuals, businesses, and governmental bodies, in order to guarantee a coordinated and group reaction to cyberattacks.

Second, governments are realizing more and more how important it is to create a safe and reliable digital environment in order to stimulate innovation and economic progress. Since a large fraction of the world's population depends on internet services, maintaining cyber resilience is essential to the survival of digital economy.

Forecasts show a significant increase in telecom income, which emphasizes the need for strong cybersecurity defences to protect digital infrastructure and increase customer trust.

This study suggests the Holistic Cyber Security Implementation Framework (HCS-IF), which aims to address these issues by offering a conceptual, logical, and methodical approach to the implementation of CSS. The HCS-IF includes flexible security measures designed to monitor the efficient application of CSSs. With the use of several high-level conceptual security controls, solutions, and procedures, the framework seeks to address the complexity of cyber threats and promote cooperation amongst different stakeholders.

The paper is organized as follows: initially, the HCS-IF is presented, outlining its main elements and guiding principles. After that, a comparative study is carried out to evaluate the effectiveness of the HCS-IF compared to other frameworks that are currently in use. In summary, the paper ends by stressing the importance of implementing cybersecurity with a comprehensive strategy and reviewing relevant literature.

2. Proposed Framework (HCS-IF):

In order to harmonize national security goals with operational imperatives, the Holistic Cyber Security Implementation Framework (HCS-IF) functions as a thorough implementation guide for Cyber Security Strategies (CSSs). CSSs are usually the result of a comprehensive revaluation of current information security environments, and the HCS-IF is well-positioned to support the achievement of these goals in implementing countries. This section explores the main elements of the HCS-IF and outlines the development process that was used.

2.1 HCS-IF Development Methodology: Creating a security framework requires a multifaceted approach that integrates aspects of science, art, engineering, and social dynamics. Although current approaches provide insightful information, they frequently fall short of offering a comprehensive solution that can be tailored to address cyber security issues at the national level.

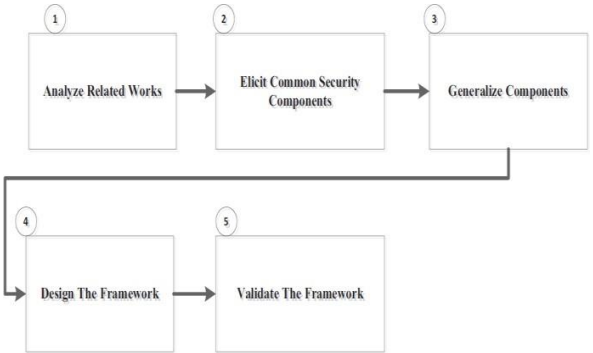

Figure: 1

The procedure used to produce HCS-IF combines knowledge from the literature research with real- world experience through a methodical, iterative approach shown in Figure 1. The essential actionsconsist of:

1. **Analysis of Literature:** Comprehensive assessment of literature on the application of cyber security strategies at the corporate and national levels, including cyber security plans, global standards, and basic frameworks for implementation.
2. **Elicitation of Common Security Features:** Thisprocess identifies the broad cyber security elements that are in line with the strategic goals, emphasizing high-level characteristics above technical details.

The process of extracting components, refining them, removing redundant information, and transforming industry-specific parts into abstract,high-level components is known as "generalization of components."

3. **Framework Development:** Sophisticated elements are theoretically included into the HCS-IF structure, mirroring a traditional processing hierarchy of "input-process-output-feedback," guided by pragmatic observations.
4. **Framework Validation:** This involves comparing and contrasting related frameworks to demonstrate proof of concept, with a focus on empirical testing in various operational contexts to provide real-world validation.

Following this methodology makes the HCS-IF a flexible and dynamic framework that can be used to handle the changing organizational and national cyber security scenario. Its iterative development methodology promotes resilience and adaptabilityto new challenges while guaranteeing alignment with strategic imperatives.

2.2 HCS-IF:

The implementation of Cyber Security Strategies (CSSs) requires the Holistic Cyber Security Implementation Framework (HCS-IF), which offers executing nations a basic road map for accomplishing the cyber security objectives outlined in their national CSS papers. As seen in Figure 2, the HCS-IF is made up of fundamental building blocks that are intended to direct the evolution of cyber security from its current condition to a desirable future one.

Key Components of HCS-IF:

1. CSS (Cyber Security Strategy): The CSS document, which summarizes the strategic vision and goals for improving cyber security, is the foundation of the framework. It acts as the directive, outlining the state of cyber security nowas well as goals for the future.

2. Requirement Elicitation: The HCS-IF carefullyexamines the CSS to extract specific requirements that are essential to accomplishing cyber security goals. These specifications act as the cornerstonesfor both strategic planning and implementation.

3. Strategic Moves: Converting requirements intopracticable steps, strategic moves are a set of intentional activities meant to improve the effectiveness and resilience of cyber security. These actions are carefully planned to close the gap between the desired and actual conditions of cyber security.

4. Controls: Sturdy controls built to oversee and record the carrying out of strategic maneuvers are integrated into the framework. By guaranteeing adherence to defined norms and reducing potentialdangers, these controls act as safety measures.

5. Security Objectives: The framework synchronizes tactical actions with the broad security goals specified in the CSS document. TheHCS-IF offers a road map for attaining targeted results and strengthening cyber resilience by outlining specific goals.

6. Framework for Implementation Repository: Serving as a centralized repository for information, tools, and best practices, the repository facilitates the administration and coordination of implementation initiatives. It givesstakeholders access to crucial direction and assistance during the execution phase.

The HCS-IF essentially plays the role of a strategic facilitator, coordinating a cogent and methodical strategy for implementing cyber security. By breaking down the CSS into practical requirements and strategic choices that are guided by robust controls and connected to cyber security goals, the framework helps executing nations effectively navigate the complexity of cyber security governance.

2.3 Cyber Security Strategy (CSS):

Governments all over the world are attempting to strengthen cyber resilience by developing Cyber Security Strategies (CSSs), a critical program based on evaluations of their own information security environments. These strategies recognize the necessity of tackling growing threats and vulnerabilities and are designed in response to the ubiquitous and transformational influence of information technology on the cyberspace realm. full guidelines outlining the country's cyber security strategy are included in CSSs. These guidelines cover a variety of information clusters to guarantee a full assessment of cyber securityimperatives.

2.4 Elicitation of Requirements:

A cornerstone of software engineering approaches is requirement elicitation (RE) (Sommerville, 2011). It is essential to the HCS-IF architecture because it converts CSS objectives into practical business and security requirements.

Interdisciplinary analytical teams are involved in this phase, which involves breaking down the CSS into needs that are both doable and understandable. The HCS-IF uses RE techniques to make sure that operational imperatives and strategic objectives are aligned. This helps different stakeholder groups comprehend the nuances of cyber security requirements.

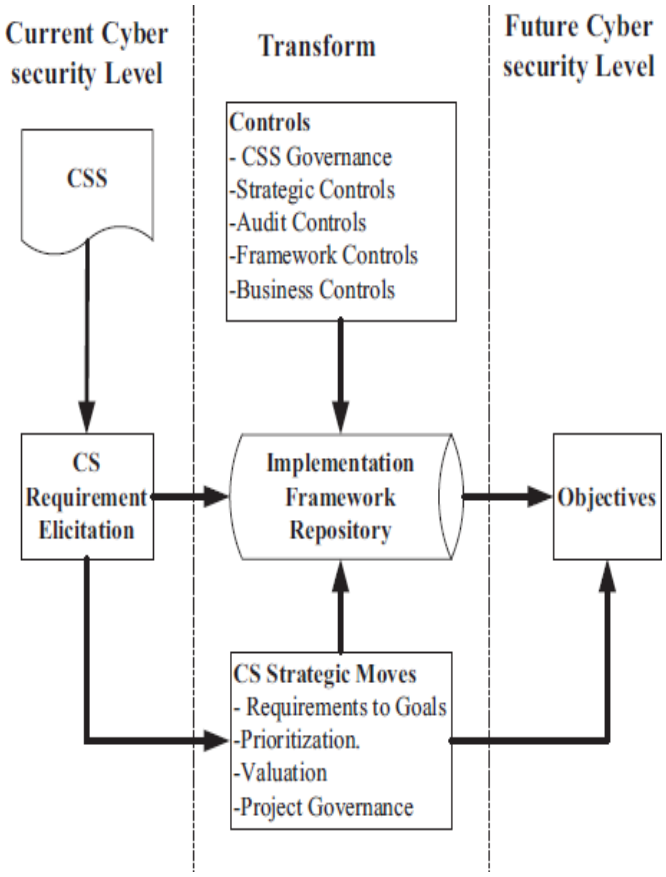

Figure: 2

2.5 Strategic Actions in Cybersecurity: Strategic movements, often known as cybersecurity moves, are planned actions taken to accomplish cyber security objectives in a specified manner. These actions attempt to complement rather than contradict one another, and are distinguished by their clarity and clear alignment with stated aims. Five different procedures are included in the strategic move's component, asshown in Figure3:

2.5.1 Change Requirements into Objectives: To enable efficient evaluation of accomplishments, requirements must be transformed into Specific, Measurable, Achievable, Relevant, and Time-bound (SMART) goals (Doran, 1981). Even though CSSs are frequently expressed in natural language, using natural language processing methods can help pinpoint possible objectives. This method incorporates subjective feedback from a variety ofstakeholders, including management, lessons learned, risk assessments, and expert opinion.

2.5.2 Set Prioritized Objectives:

Objectives are ranked according to importance,taking into account variables like deadlines, budgets, dependency requirements, and management preferences. One method is to rankthe criteria in order of significance and then weight each aim in relation to these criteria.

2.5.3 Security Valuation:

The security appraisal process determines whether initiatives that are in accordance with achieving predetermined objectives get started.

This process ensures that only projects that havethe backing of management are carried out.

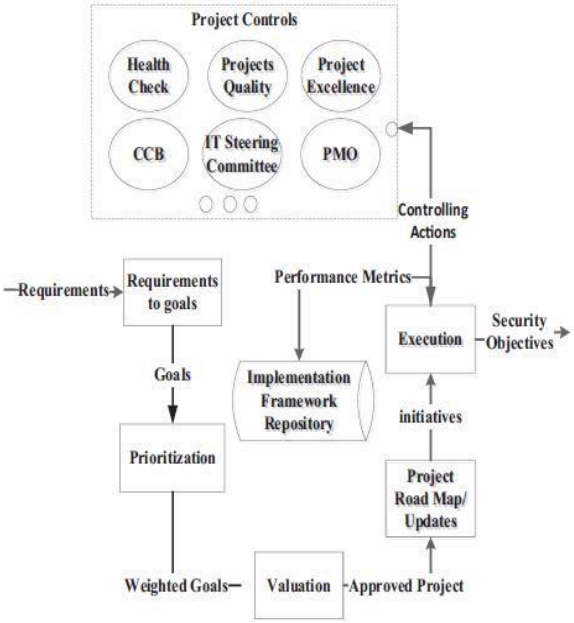

Figure: 3

2.5.4 Build/Update Project Roadmap:

The process of developing a project roadmap comprises prioritizing projects based on cost and payback. Sequencing for interconnected projects is determined using methods like project assessment and review methodology charts (Schwalbe, 2010).

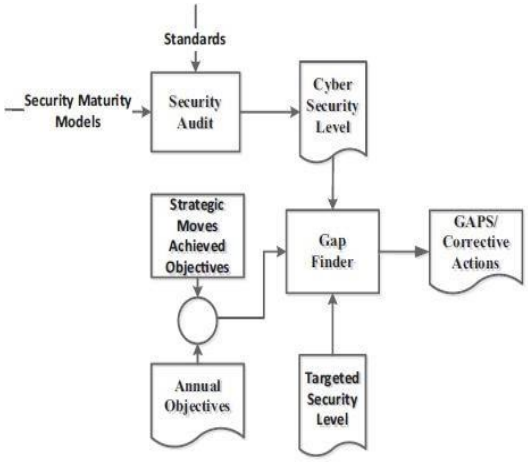

Figure: 4

2.5.5 Execution of Project Roadmap: Implementing the project entails producing concrete results and documenting metrics in the HCS-IF implementation repository. Project controls that attempt to achieve security objectives, such as Quality Assurance systems, Project Management Offices, Steering Committees, Change Control Boards, and ProjectExcellence efforts, regulate this process.

To put it simply, the HCS-IF's strategic manoeuvres make it easier to carry out cyber security measures in a methodical manner whilemaintaining alignment with overall goals and efficient management of implementation activities.

2.6 Controls:

Controls are essential tools for directing organizational behaviour and streamlining the execution of cyber security projects. They also provide decision-makers with the ability to take preventative or remedial action as necessary. Theseveral sorts of controls that are essential to the HCS-IF framework are outlined in the following subsections:

2.6.1 Controls for Governance:

The establishment of a Cyber Security Agency (CSA) with the responsibility of carrying out and supervising implementation efforts is necessary as governance controls play a crucial role in managing the implementation of CSS. The enforcement of a formalized chain of command between participating entities is guaranteed by the CSA. The three main components - CS Performance Management Control, Regulation Regime Control, and International Cooperation Control—are meant to maintain command integrity, uphold security rules, and encourage international cooperation in threat monitoring.

2.6.2 Strategic Controls:

The adoption of CSS inside the HCS-IF framework is contingent upon the deployment of strategic controls by the CSA. These controls provide decision-makers the authority to assess how effectively objectives are being fulfilled and to take swift action. Strategic controls should be adaptable enough to vary with the demands of the CSA and adapt to corporate culture. These controls should address issues like quality, monitoring, incentives for human resources, performance assessment, and vigilance.

2.6.3 Controls for Audits:

Audit controls provide two functions: they assessthe system's security maturity levels and find security flaws in the CSS document or implementation process. As part of security maturity level evaluations, ongoing implementation efforts are inspected against specific security standards, and gaps are found bycontrasting the current and intended maturity levels. This process suggests corrective actions, which enhances the implementation roadmap.

2.6.4 Framework Controls:

In order to manage the HCS-IF technique and maintain its efficacy and relevance over time, framework controls are necessary. These controls include resilience management, access control, recovery management, universal

standard compliance, version control, configuration management, and framework repository management. These restrictions become especially important when automated CSS implementations are made with the help of the HCS-IF in Tools forComputer-Assisted Software Engineering (CASE).

2.7 Controls for Businesses:

Business controls are crucial for operational effectiveness but fall outside the scope of this paper. Examples include regulatory management,international cooperation, recovery management, incident management, human resource management, vendor management, commitment plans, change plans, awareness initiatives, and capability building. To be thorough, we include aquick mention of these here.

2.8 Cyber Security Objectives:

In accordance with the CSS, the CSA implements necessary measures to accomplish long-term goalsrelated to cyber security. These goals are divided into annual goals to enable continuous evaluation and monitoring of HCS-IF performance.

Comparison with achieved targets aids in strategicdecision refining and ensures alignment with overall security goals.

In summary, the broad range of controls present inthe HCS-IF framework ensures a systematic and structured approach to cyber security implementation, encouraging adaptability and resilience in the face of evolving threats.

3. Validation of the Proposed HCS-IF:

While there are a number of security frameworks available for safeguarding cyberspace, many of them are exclusive to certain entities or areas and only apply at the national level. As demonstrated in Sections 4.3, there is a discernible deficiency in the accessibility of a thorough framework for implementing Cyber Security Strategies (CSS) at the national level. The Holistic Cyber Security Implementation Framework and other existing frameworks, which are divided into six categories and listed in Sections 4.1 through 4.6, interact with common goals of enhancing security and streamlining implementation processes. Notably, the HCS-IF serves as a thorough and complete approach to putting cyber security into practice. It is designed to complement and improve existing frameworks rather than to completely replace them.

3.1 Comparison Criteria:

A predetermined set of features, obtained from research ideas and literature reviews, is used to compare the framework to current ones. These characteristics address the shortcomings of current frameworks and provide the main driving forces behind this study. Subjectively, each characteristic is evaluated in relation to the framework, listed between Sections 4.1 and 4.6:

Resilience: Indicates how easily and adaptably the framework can adjust to unanticipated changes in the environment, technology, and attack techniques.

Measure Performance: Assesses how well the framework works to gauge how well security activities are performing at all organizational levels.

Compliance: Evaluate how well the framework manages standard deviations and conforms to established standards or best practices.

Measure Security Level: Establishes the framework's capacity to express the level of security attained at any given moment.

Find Any Gaps in the CSS Document: This section looks at how well the framework can findany weaknesses in the CSS document that need tobe fixed in order to achieve the required security levels.

Level of Implementation: Takes into account whether the framework is appropriate for nationalimplementation, in keeping with the all- encompassing strategy that Trim and Lee (2010a) and Dasgupta and Rahman (2011) support.

Table I summarizes the frameworks that were analysed, and the suggested HCS-IF stands out as a top option because of its all-encompassing design that is specifically suited for the implementation of cyber security. Crucially, rather than attempting to replace current frameworks, standards, and methodologies, the HCS-IF is made to work in concert with them to accomplish a thorough application of cyber security.

All things considered; the HCS-IF is a big stepforward in tackling the intricate issues surrounding cyber security governance at the federal level. It provides a strong and flexible framework for boosting cyber resilience and protecting vital infrastructures.

4. Related Works:

To aid in systematic study, the relevant material isdivided into discrete logical categories that acknowledge their interconnectedness:

4.1 Management and GovernanceFrameworks:

A lot of frameworks concentrate on information security from a management standpoint. Notable examples include Zuccato's enterprise security management framework mapped with the system security engineering maturity model, Janssen andHjort-Madsen's national enterprise architecture framework. All three emphasize the bigger governance perspective in enterprise architecture.

4.2 Guidelines:

International information security programs often contain guidelines to enhance implementation efforts. For instance, advocate an awareness toolkit for the implementation of South Africa's strategy, whereas the Estonian Department of Defence (2008) suggests a phased deployment overseen by government organizations and security providers.

4.3 Dedicated Frameworks:

Specialized frameworks are designed to meet the security needs of specific countries or organizations. Examples include the Jordan CSS implementation framework proposed by Otoom and Atoum and the ongoing research being carried out by the Integrated Governance, Risk and Compliance Consortium to safeguard the United Kingdom on threat monitoring and control status updates.

4.4 Generic Frameworks:

Although they may focus more on business strategy than cyber-security, generic frameworks for strategy execution, as those put out by Barnat(2005) and Trim and Lee (2010b), offer flexible techniques adaptable to diverse circumstances.

4.5 Frameworks Specific to Providers: Provider-specific frameworks—such as the Oracle® Reference Architecture (ORA) and the IBM® Security Framework—offer customized reference architectures and implementation recommendations for security solutions inside their own ecosystems (Buecker et al., 2010; Oracle®, 2011).

4.6 Frameworks for Open Architectures: Numerous enterprise architecture (EA) frameworks provide thorough models for comprehending organizational structures and procedures, such as Zachman, Federal Enterprise Architecture Framework. These frameworks help answer basic "what" questions and offer insightful information on integrating security into larger architectural contexts.

To sum up, the numerous related studies highlightthe complexity of cyber security governance and execution, with each framework offering unique perspectives and methods appropriate for certain situations..

5. Final thoughts and next studies:

A comprehensive and well-structured Cyber Security execution Framework (HCS-IF), designed to facilitate the comprehensive implementation of Cyber Security Strategies (CSSs), is presented as the study's conclusion. CSS, requirement elicitation, strategic movements, controls, security objectives, and framework repository are essential components ofthe HCS-IF. Together, these components make it easier to translate CSS requirements into tactical moves that may be used to accomplish security goals. Comparing the HCS-IF to the six suggested framework categories makes it evident that the HCS-IF outperforms the others due to its comprehensive approach to cyber security implementation.

This paper makes a substantial contribution by providing possibilities for future research, including expanding the framework to include additional elements like global governance, organizational structures, human resources, and regulatory regimes. Furthermore, investigating governance options other than the Cyber Security Agency (CSA) that has been proposed could provide insightful information. Further study in this area is required to evaluate the efficacy and reliability of the HCS-IF through practical testing. Moreover, research should be done on the creationof a Because it has the potential to enhance CSS implementation, the HCS-IF is a crucial component of a Computer-Aided Software Engineers (CASE) tool.

To sum up, the HCS-IF that has been suggested provides a thorough framework for the implementation of cyber security and opens the door for further research projects that will improve and refine cyber security tactics worldwide. The field of cyber security can gain from improvements in strategy implementation procedures by tackling these areas of future research, which will ultimately promote a safer and more secure digital environment for all partiesconcerned.

6. References:

1. Accessible at http://linkinghub.elsevier.com/retrieve/pii/S13613 72309700612, Broom, A. (2009), "Security consolidation and optimization: gaining the most from your IT assets," Computer Fraud and Security, Vol. 2009 No. 5, pp. 15–17(retrieved February 25, 2012).
2. "Introducing the IBM security framework and IBM security blueprint to realize business-drivensecurity," by A. Buecker, M. Borrett, C. Lorenz, and C. Powers (2010), IBM Redpaper, Vol. 4528No. 1, pp. 1-96.
3. "A framework for estimating security coveragefor cloud service insurance," Dasgupta, D., and Rahman, M. (2011). Published by ACM Press, New York, NY, USA, in Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research, p. 40. Accessed April 20, 2012, via http://dl.acm.org/citation.cfm?doid 2179298.2179342.
4. Available at www.malone.edu/media/1/39/480/MMP405_Onli ne_Corporate_Strategy.pdf (accessed February 12,2012), David, F. (2011), Strategic Management: Concepts and Cases, 13th ed., Prentice Hall.
5. Doran, G.T. (1981), "Writing management goals and objectives can be done in a SMART way," Management Review, Vol. 70, No. 11, pp.35-36.
6. EAdirections (2013), EA Frameworks: Benefits and Drawbacks - Catalog and Perspectives. Available at www.eadirections.com/uploads/EA_Frameworks_Pros_and_Cons.pdf is Report EA-7004.
7. Enterprise Information Systems, Vol. 4 No. 2, pp. 111-136, Erol, O., Sauser, B.J., and Mansouri,

M. (2010), "A framework for investigation into extended enterprise resilience," accessible at www.tandfonline.com/doi/abs/10.1080/17517570903474304

Cyber Security Strategy-Estonia, published by theEstonian Department of Defence in 2008, can be accessed at www.mod.gov.ee/files/kmin/img/files/Kuberjulge oleku_strateegia_2008-2013_ENG.pdf on February 1, 2012.

9. Fielden, K. (2011) International Journal, Vol. 4No. 1, pp. 427–434 "A holistic view of information security: a proposed framework".
10. The "Cyber Security Strategy" published by the Australian Government in 2009 can be accessed at www.ag.gov.au/RightsAndProtections/CyberSecu rity/Documents/AG Cyber Security Strategy-for website.pdf (accessed July 2, 2014).
11. "A framework for security requirements engineering," Haley, C.B., Moffett, J.D., and Laney, R. (2006), Proceedings of the 2006 International Workshop on Software Engineeringfor Secure Systems, ACM, pp. 35–42, accessibleat http://dl.acm.org/citation.cfm?id1137634

(retrieved February 21, 2012).

12. HM Government (2010), The National Security Strategy, A Strong Britain in an Age of Uncertainty, The Stationery Office, www.official-documents.gov.uk/ (accessed December 23, 2011).