Developing and Measuring a Cyber Security Architecture Course – A Case Study

Dr. Dennis H. McCallam
2691 Technology Drive
Annapolis Junction, Maryland
USA

dennis.mccallam@ngc.com

ABSTRACT

The United States National Initiative for Cybersecurity Education [1] points out not only the lack of qualified cyber security personnel, but also the lack of realistic education to help train the next generation of cybersecurity. The issue of enhancing cyber education and training to produce cybersecurity engineers has been recognized both as a problem and a solution [2], [3]. Northrop Grumman understands that criticality and established the Cyber Academy, chartered to be the educational conduit for both internal Northrop Grumman personnel and our broader customer base. The need for education that provides the right cybersecurity skills, at an accelerated pace, to defend against the sophisticated cybersecurity threats is widely supported [2], [3], [4], [5], [6]. Where this becomes important is in developing the proper courses for education. This paper presents a course that was designed to address the education need and describes not only the curricula, but also the experiential learning the course used as context and then presents a quantitative and qualitative analysis of the impacts of the course from the student perspective. These results were taken immediately after the course and then again in a 5 month follow up session to gauge overall retention and application.

1.0 WHAT WAS THE PROBLEM SET?

There were in fact two problem areas that were being addressed: the education and growth of cyber architects and gaining repeatability in design as a course outcome. The initial problem is in the area of cyber education and training that accelerates the growth of experienced cyber architects. Looking at cyber from either an art or science standpoint, Ref. [7] asserts that cyber science and engineering; focusing on the design, development and deployment of cyber defence; is weak or almost non-existent. The Deputy Assistant Secretary of Defense for Cyber, Identify and Information Assurance [2] points out the importance of developing the cyber security workforce through training. Cybersecurity capabilities must move away from stove-piped approaches to cyber defence and be "designed and synchronized through enterprise architecture, enterprise systems engineering, a focused technology pipeline, and active portfolio management" (p.8). Providing architects with proper training and tools to help them design and implement cybersecurity therefore becomes important. The (United States) President's Comprehensive National Cybersecurity Initiative states education and training are critical to developing the cyber workforce.

Research is needed in a myriad of areas with respect to education and training. For example; how effective is training on the workforce with respect to improving the network defence; what is the most effective way of providing cyber training and education; or can cyber architecture approaches be operationalized. The specific interest area is in cyber security architectures, particularly for how they can be operationalized as a repetitive process producing consistent artefacts to measurably improve cyber security defences. Additional educational emphasis in cyber security, particularly with advanced topics would add value to existing IT programs [15].

Additionally, they stress that a cyber-security curricula needs to address the ability to communicate solutions to technical and non-technical audiences.

The second problem area is providing a set of repeatable cyber security solutions and artefacts that could allow practitioners to communicate a solution. The implication is to better know when an enhancement (better training, a new technology, an additional process, etc.) is robust enough for operational deployment and what defines, for solution providers, a "customer ready" enhancement for integration. Cyber architecture is an emerging area that is bringing systems engineering discipline into information assurance systems. Ref. [8] discusses the paradigm shift from reactive security solutions to more adaptive strategy that balances business requirements while still implementing effective security controls. Ref. [9] offers a method of evaluating information assurance approaches that relies on weighting factors for competing solutions with the weighting factors agreed upon by the stakeholder – decision makers. While this approach is good for individual systems, this does not allow for easy repeatability of solutions across domains unless the weighting factors are nearly identical in the different domains.

Ref. [4] states that keys to accelerating the growth of systems engineers relies on systems thinking approaches coupled with experiential learning. While this is related to the previous problem on cyber education, experiential learning also is a fundamental element of making practical implementations. SABSA [10] leverages the Zachman enterprise architecture approaches and describes a consistent and proven process that results in a system specific architecture and architecture artefacts. While the process remains constant, the results are challenging to compare due the results being to being system and stakeholder specific and produces visuals that are difficult to reconcile between systems. An overall weakness of both SABSA and Zachman, is the inability to develop attributes (patterns) that can be modelled or measured.

2.0 SELECTING THE EDUCATIONAL USE CASE

This would be constructing curricula to solve the problem set, but how best to do this became the next issue to address. Experiential learning is education that utilizes real world systems and examples are important not only to reinforce concepts but most importantly to provide context. This is supported in the literature in a number of research activities. Ref. [13] claims an effective cyber course contains interesting assignments, connects to job functions, and involves increasingly more complex and real life problems as exercises. Ref. [14] stresses the need to include global level security problems within the curriculum. Ref. [15] makes the point that case studies are an effective way of proving education, particularly for linking real world events and cyber events. They suggest additional emphasis in cyber-security, particularly with advanced topics that would add value to existing IT programs. The issue then became selecting a system that was both realistic and meaningful.

Ref. [17] provided the analysis of the Automated Computer Network Defence (ARMOUR) system that satisfied two concerns: first that the information about the system was freely available and second that the system satisfied the "real world" contextual requirement. ARMOUR became the exemplar chosen. As described both the ARMOUR RFI [33] and the analysis of Sawilla and Wiemer, ARMOUR provided a rich area for utilization as an architectural study artifact. The following overall view of ARMOUR is from the ARMOUR RFI - "Defensive actions (e.g. remove a network route, shut down a service, or apply a virtual patch) must be taken either proactively or, at the very least, at a speed capable of mitigating attacks. ARMOUR will demonstrate the capability to proactively deal with vulnerabilities and reactively mitigate ongoing attacks in real-time. ARMOUR will demonstrate the capability to automatically generate optimized courses of action (COA). Proactive COAs will minimize the risk of attacks on the networks while reactive COAs will allow operators to react more quickly to on-going attacks. The focus of the ARMOUR Technology Demonstration Program project is to deliver an integrated and automated demonstration system that will:

- Compute defensive COAs in response to identified cyber security vulnerabilities and attacks;
- Prioritize cyber security defensive COAs to minimize cost and impact to operations;
- Proactively and reactively respond in a semi-automatic (man-in-the-loop) or fully-automatic manner; and
- Compute system security metrics over the entire system to enable comparison of previous and potential cyber security network states."

3.0 STRUCTURE OF THE COURSE

Now that the exemplar system was chosen, the course was constructed. The target audience of this course are those security architects who develop and design security architectures and who provide and/or develop any or all of: security strategies, security capability maps, as-is/gap/ life cycle analysis for security functions, overall security portfolio strategies, security application diagrams, system maps, security/service/technical interfaces, and security integration strategy. In their research, Ref. [18] examined and evaluated position descriptions and determined that security architects typically hold bachelor's degrees and have 5 or more years of experience but seldom hold managerial positions (p. 298). We performed a similar review and examined position descriptions listed on both http://jobview.Monster.com/ and http://jobs.ISACA.org/ for cyber architects. This not only corroborated the analysis by Ref. [18], but also yielded enough consistent information to draw some conclusions about the characteristics of the cyber architect population. The common traits were:

- Understanding of architecture and design of secure solutions (in some cases using definitions of confidentiality, availability, and integrity).
- Ability to interpret and develop security requirements.
- Critical thinking and the ability to communicate and defend architecture.
- Knowledge of security standards.
- Production of artifacts such as gap analysis, threat assessments, technology assessments, and test cases.
- Understanding of the systems development lifecycle.

Combining the results from Refs. [18] and [10], primary job descriptions and roles in the population of cyber security architects for the purposes of this research can be defined as:

- Architect, implement, and integrate technical cyber/cyber security solutions, hardware, software, and services.
- Understand and be able to apply cyber security standards (such as NIST 800-53 and NIST 800-37), directives, guidance and policies to an architectural framework.
- Develop artifacts that represent the security architecture.

The intent was to have students (cybersecurity engineers) who attend the course gain the following outcomes:

- Apply cybersecurity architecture pictorial views (technology, capabilities, requirements, gaps);
- Develop repeatable architectural descriptions and artifacts that can be utilized for concept evaluation, capability analysis, proposals, project development, and final reports; and
- Learn to transform an existing system to accommodate cybersecurity requirements or develop a new cyber-enabled solution.

Topics within the course included the relationship between systems engineering and cybersecurity engineering, the growth of enterprise architecture [12], [16], [20], and how system security architecture developed from enterprise architecture [10], [11]. The architecture course also includes exercises in producing cybersecurity architecture pictorial views (artefacts) that can be reused and shows how the artefacts can be used for requirements analysis, technology placement on cybersecurity defences, cybersecurity capabilities, as-is and to-be analysis of cybersecurity capabilities, and potential strengths/weaknesses of cybersecurity capabilities.

The course avoided employing architectures and processes that resulted in a disparity of views, such as DoDAF, The Open Group Architectural Framework (ToGAF) and Zachman. There were two reasons for this. Ref. [19] points out that none of these processes were designed for or provide for information security and all provided for views but the processes utilized resulted in views that are system specific [20]. Four architectural views are used in this course representing different facets of architecture: the SANS Critical Security Controls (CSC), the Fan™, CyCape™ (cyber capabilities view), and the NATO Cyber Defence Capability Framework. These views are relatively independent of the systems they describe and provide a means to compare solutions from different systems [21]. The course employed four architectural views representing different facets of architecture: SANS Critical Security Controls (CSC), the Fan™, CyCape™ (cyber capabilities view), and the NATO Cyber Defence Capability Framework. These views are independent of the systems they describe and provide mechanisms to compare solutions from different systems, unlike traditional enterprise architecture approaches.

The course has eight individual learning modules along with five exercises and is presented over a two-day period. The course showed students how to develop repeatable cyber solutions based on sound architectural fundamentals and systems engineering principles in order to consistently communicate solutions to stakeholders and strengthen defences against the cyber threat. The course provided an understanding of cyber architecture; what it is and why it is important; the role of cyber architects; and introduced various cyber artefacts, capabilities, and frameworks.

Modules One through Three provided an introduction to cybersecurity architecture; examine cyber architecture drivers (in terms of policies, requirements, and laws), and security controls as defined by NIST. Module Four focuses on the SANS Critical Security Controls (CSC), and its use as a cyber architectural artefact. The key objectives are to recognize how the SANS CSC diagram (Figure 1) can be utilized as a baseline security configuration artefact, can be used as a rating mechanism, and how that artefact provides a cybersecurity defensive architecture view.

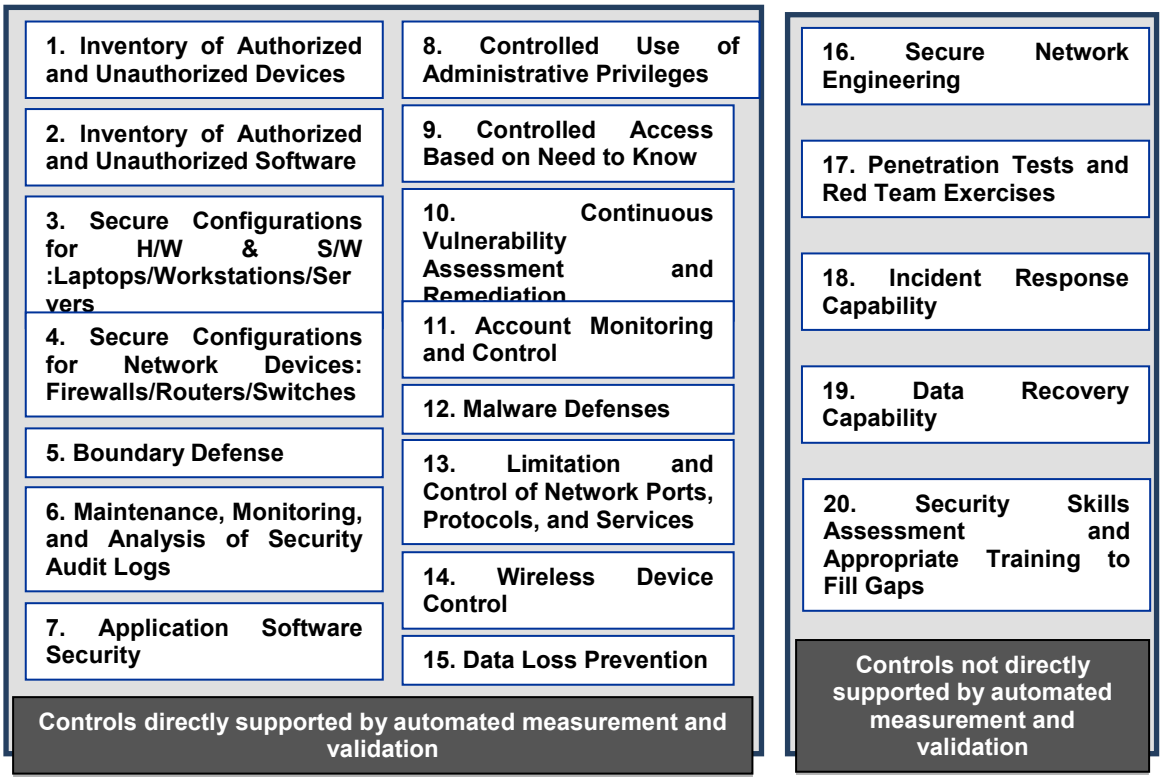

Figure 1: SANS Critical Security Controls Presented as the Twenty Control Areas Illustrating the Artifact View.

Module Five presents the second framework known as the Fan™ a cybersecurity defensive analysis framework and visual architecture view developed by Northrop Grumman Corporation and shown in Figure 2.

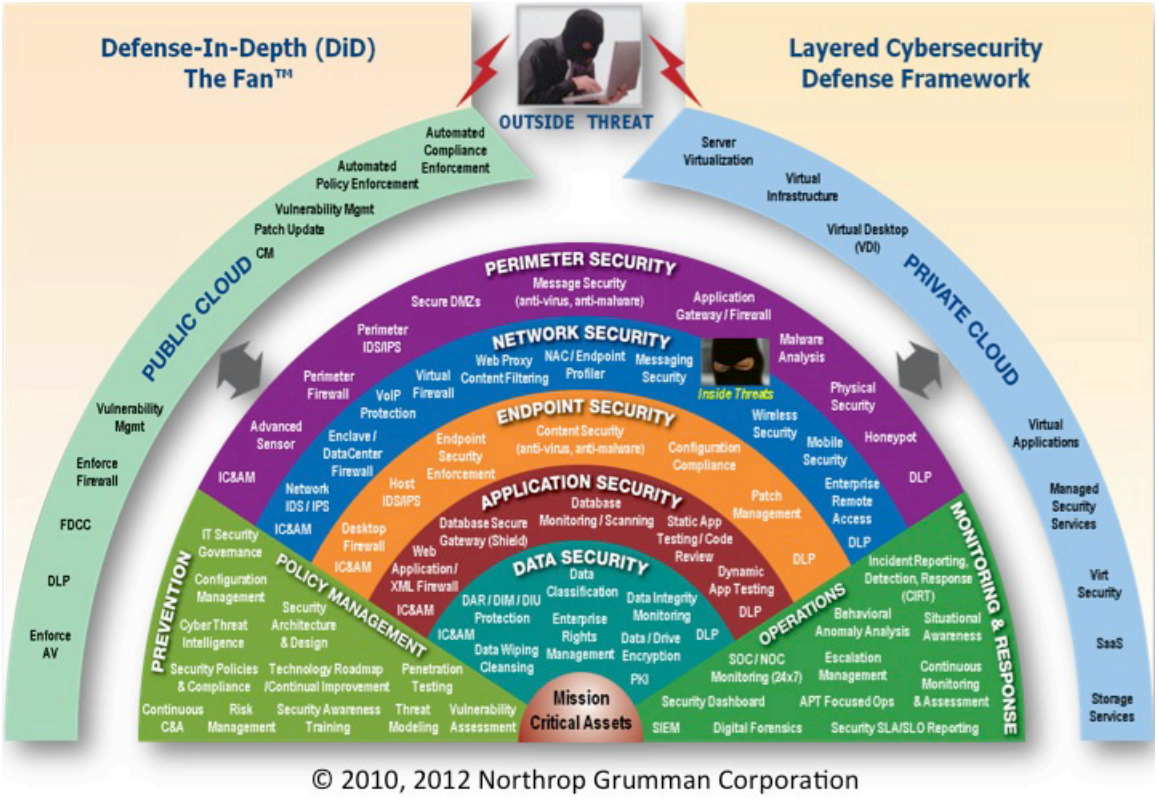

Figure 2: The Fan™ Illustrating Technology and Process Defence in Depth Architectural Pictorial View. Copyright 2010, 2012 by Northrop Grumman Corporation. Reprinted with permission.

Module Five explains how each layer of the Fan™ represents aspects of a cyber defence-in-depth approach; how the technologies and processes related to each layer of the Fan™ and each layers contribution to an overall cybersecurity defensive profile; and to understand how the Fan™ artefact can be used in an iterative process for developing a cybersecurity architecture view.

Module Six describes the CyCape™, a cybersecurity defensive analysis framework and visual architecture view developed by Northrop Grumman Corporation and is shown in two parts in Figure 3 and Figure 4. This module examines the CyCape™ framework, its utilization as a view and the key cyber capabilities described in the CyCape™ model and how the CyCape™ artefact can be used in an iterative process for developing cybersecurity architecture views for capabilities, gaps, and requirements.

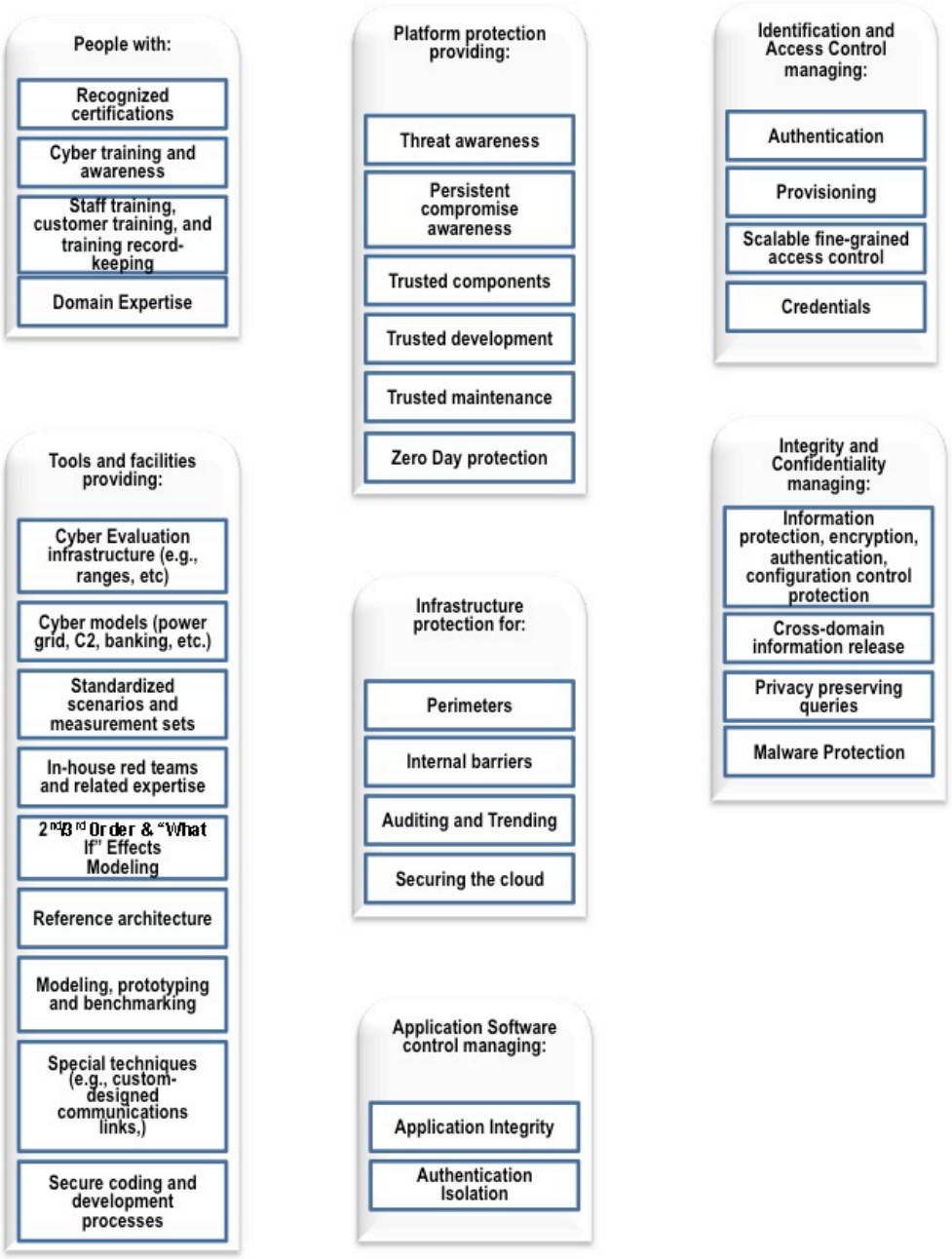

Figure 3: CyCape™ First Seven Components Illustrating Technology and Process Defence in Depth Architectural Pictorial View.

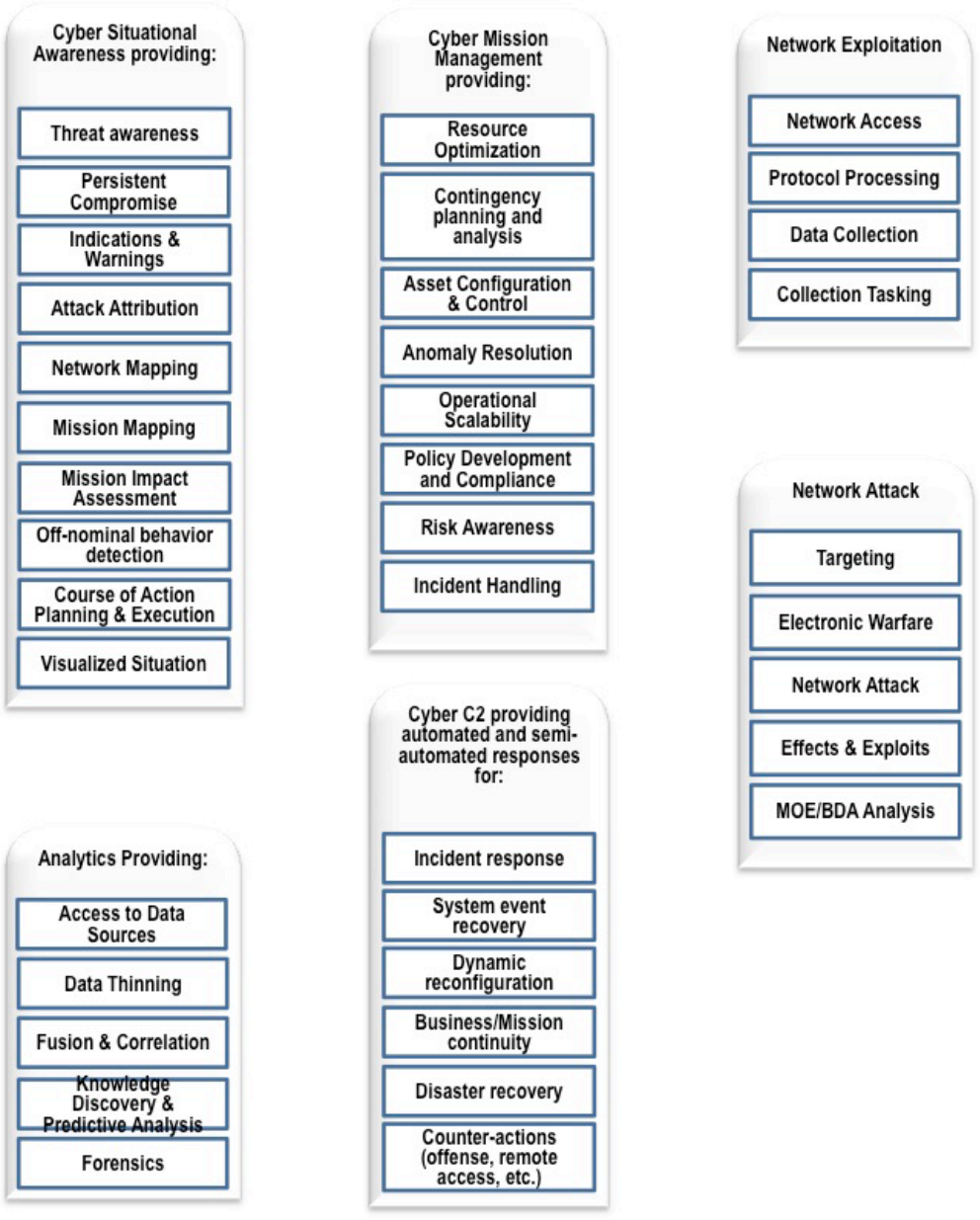

Figure 4: CyCape™ Final Six Components Illustrating Technology and Process Defence in Depth Architectural Pictorial View.

Module Seven describes the NATO CIS Security Capability breakdown (Version 2.0) as a cybersecurity defensive analysis framework and visual architecture view as illustrated in Figure 5. The NATO module explains: the purpose of having a multinational framework in the development of cyber defence capabilities; defines key NATO Information Assurance (IA) terminology; and how the framework can be used in an iterative process for developing cybersecurity capability views for capabilities, gaps, and requirements.

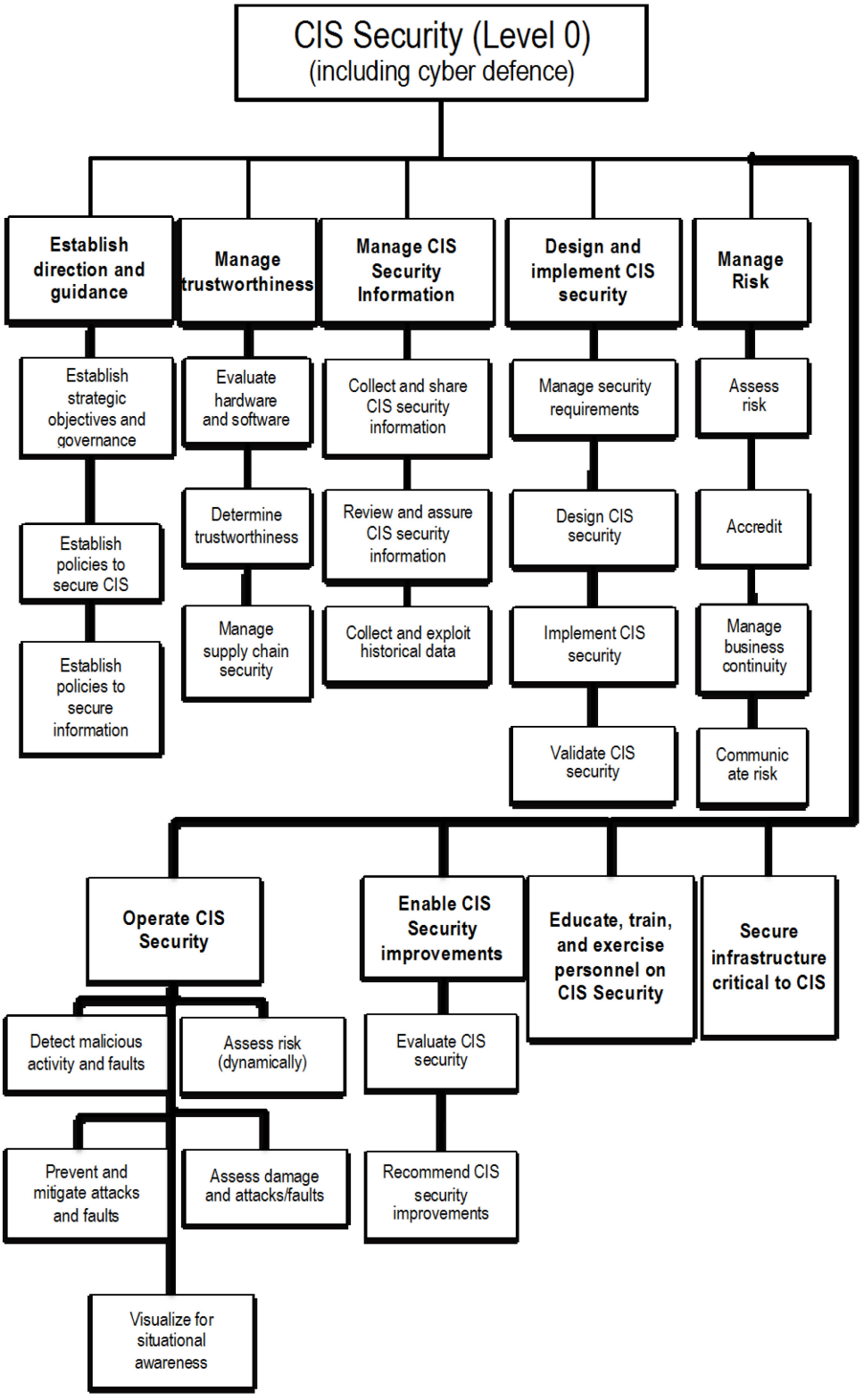

Figure 5: NATO Cyber Defence Capability Framework Showing First and Second Level Breakdown.

Module Eight is a real world example that breaks down the ARMOUR systems and demonstrates how to implement the artefacts and illustrates to the students how to apply all the information taught in the class. The specific case study illustrates how to decompose that set of requirements, map those requirements to the four framework artefacts, and then provide meaningful summaries.

There are also five specific exercises that form part of the training where the students demonstrate knowledge and implementation of the concepts covered. The exercises are performed in teams where the groups present their findings to the entire class with the class acting as the stakeholder customer, where the stakeholder customers can ask questions and probe into the reasoning behind each answer. From a learning perspective it consists of analysis of the problem, understanding and application of the learning material, and creation of the final report to the customer identified in the problem description.

4.0 OUTCOMES BASED LEARNING

Ref. [6] discusses outcome-based education where the expectation of the learning or the outcome, is clearly discussed with the learners in the beginning of the education. They further define the concept of specific outcome that demonstrates learning and mastery of a skill. The architecture learning and development course clearly states all the objectives. The course objectives are stated during the course introduction and reinforced throughout the course at the beginning of each module. In addition, the exercises provide a mechanism for the cybersecurity engineer student to practice and demonstrate a level of understanding of the desired competencies. Ref. [22] discusses the concept of competency–driven instruction that stresses tactical knowledge teaching; or those facts, principles, or skills that are required in the decision making process of using a learned topic. The architecture course is competency-driven in design, as one of the goals is to increase availability of cybersecurity engineers to perform cybersecurity architectural assignments. In addition, this goal supports the systems thinking movement that seeks to decrease the time it takes to develop cybersecurity systems engineers [5], [4].

5.0 INITIAL RESULTS ON EFFECTIVENESS AND FINDINGS

Testing was done on the first 3 classes utilizing a before and after quantitative survey instrument that included some qualitative questions for the post-course analysis. Results were processed for only those students who attended all of the class and completed the exercises. There were 75 students in the three classes. Of that number, 63 students (52 technical and 11 management) completed the class. The quantitative data collects information from the cybersecurity engineer students on the course in terms of being relevant to their job and their perceptions on the usefulness of the subject matter presented all measured utilizing a Likert scale. There is also some demographic related information on years' experience, cyber certifications held, gender/age. The qualitative part of the survey asks open ended questions on what students liked most, liked least, their comfort level with ability to utilize the material, and missing expected information.

In particular, two questions from the post-course survey asks the students to quantitatively rate perceived knowledge of subject matter before/after the course, and two questions students to quantitatively rate perceived ability to implement the knowledge both areas using a 1 – 10 Likert scale. The overall results were a perceived knowledge increase of over 30% from prior to taking the class. But the real improvement is increasing the number of more confident engineer-architects. This addresses the needs of NICE in terms of developing new cybersecurity learning curricula and successfully deploying. The cybersecurity architecture approaches supports the systems thinking findings from [5], [4] that emphasize the need to accelerate the development of senior systems and by extension senior cybersecurity engineers. Finally, the curriculum was developed to leverage the impact of experiential learning in utilizing real world scenarios as the primary source of exercises [23]. Figure 6 summarizes the key findings.

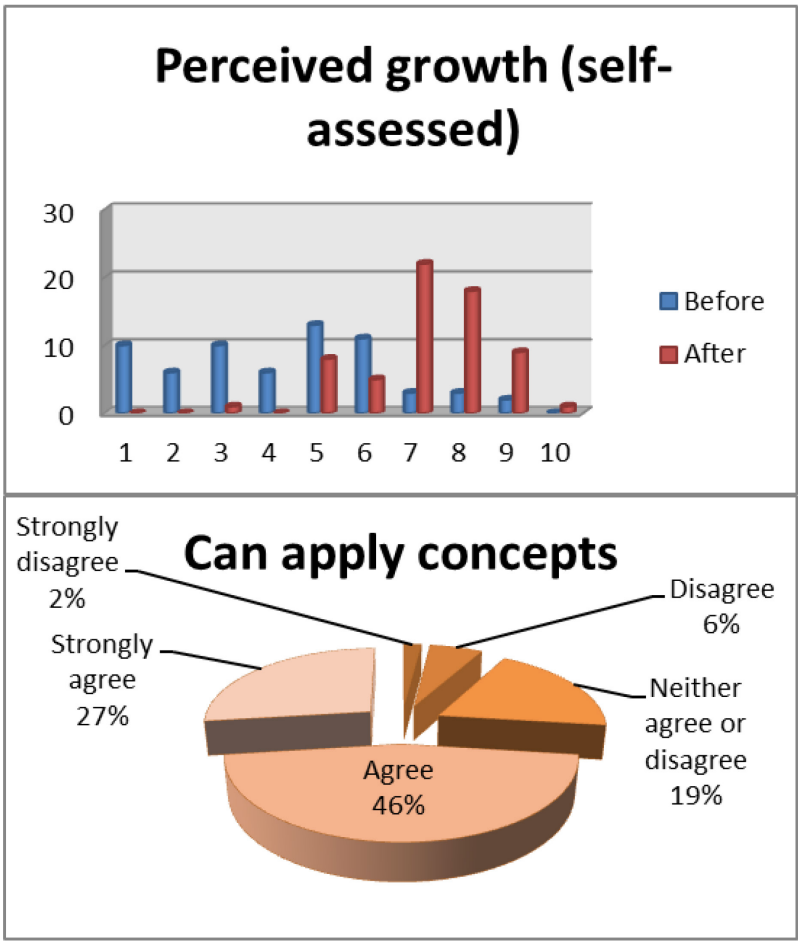

Figure 6: Key Findings from the Analysis.

The qualitative responses were even more telling. There were some strong feelings presented. One student liked the idea there are 4 different models that allow us to present architecture from different vantage points. As far as improvement on knowledge, we heard confident comments such as "I believe I could assist on a team; whereas prior to the course I did not have the knowledge, framework or tools to do so" and "I'll use the concepts". Some were less confident, but even the remark "Not ready to be lead, yet" indicates overall desire to get to that point. As far as the exercises are concerned, the "real like examples were helpful".

The overall findings of the study identified four primary themes. These are an inconsistency in current cybersecurity architecture practices, that the solution studied in this research satisfies in principle Levels 1, 2, and 3 of the Kirkpatrick model, there is evidence to support a claim that the solution addresses Level 4 of the Kirkpatrick model, and the solution advances the state of the practice with respect to cybersecurity architecture and systems thinking. The case study conducted by this research satisfies all aspects of trustworthiness: confirmability, dependability, transferability, and credibility as described in section 3.5.

Ref. [24] studied the crossover between enterprise architecture and information assurance (cybersecurity). They pointed out that neither frameworks nor enterprise architecture addresses information assurance. The research findings strongly support those conclusions, specifically that previous processes for cybersecurity architecture

were mostly ad hoc, self-taught, and were perceived by the subjects to be inconsistent. The uniformity of the comments by the students and the use of NVivo indicate confirmability and consistency of the data [25], [26]. Student 2 gave perhaps the best explanation. "It depended on if the customers had specific requirements in a lot of cases, some of it was trial and error, some of it was mandated DISA STIGS, some of it was things we've been taught in some of the other cyber courses, on the job training from mentors of various sorts when we came up with questions. It was a collection of different things, some of which were ad hoc". When asked directly about the process being consistent or adaptive, Student 6 said "adaptive, based on the clients needs". Student 3 provided a succinct summary of previous approaches. "We need a standard way of approaching this area. The requirement is not to have the same answer every time, but to take a consistent approach and be able to have everybody understand that consistent approach." That last comment validates the claim that cybersecurity engineers lack a systems engineering background that brings with it consistency and structure [23].

Second, the cybersecurity architecture course solution is a valuable course per the Kirkpatrick model and evaluates favourably against the first three criteria of the Kirkpatrick model. Levels 1 through 3 of the Kirkpatrick model refer to the student's perceptions on favourable reaction to the training, perceived learning because of the training, and actual use of the training in a daily job situation [27]. The research showed clearly that the proposed solution course on cybersecurity architecture was well received by the students. The reactions to the course were consistently positive across all the interviews. Student 2 indicated the course was "very useful", as did Students 4, 6, and 7. A key comment on favourable reaction came from Student 3 who indicated the "course process normalized ad hoc processes" and that "it gave structure and order to my thinking". There are skills and competencies within the cybersecurity architecture course that can be learned and all students perceived learning from this experience. Student 1 provided a key observation by stating "Now having taken the course, I can look back and see that some of the assumptions that were made and some of the decisions that were made were not as good as they could have been". The comments also referred to now having a more standardized and organized approach to learning about cybersecurity. Perhaps the salient comment came from Student 6, who definitively stated learning "I learned a lot". The learning was further supported through commentary on the exercises where Student 7 indicated about the exercises, "I definitely learned more than from reading or seeing".

Third, the use of views resonated with customers to the point that there might be a little support for approaching the level 4 Kirkpatrick criteria of economic impact. Level 4 of the Kirkpatrick model focuses on the benefit, in terms of impact to the organization, and is typically measured financially [27]. "Most training efforts are incapable of directly affecting results level criteria" [28]. While there was no measured economic gain or intent to measure economic gain, all students who used the concepts from the cybersecurity architecture course in customer interactions and briefings reported favourable customer feedback. Student 1 keyed in on a topic that does have some level of economic impact in terms of a discriminator "I find this to be a real differentiator and a real discriminator, and clearly the customers I talk to at any level see it same way. We're connecting the dots and the customers see real value in it." Student 2 used the concepts in the course and prepared a customer briefing illustrating the potential customer cybersecurity solution. The comment was "it went over real well". And in a related setting, academia, Student 5 used the concepts from the cybersecurity architecture course in their academic Master degree program. That student stated, "Considering the teacher gave me 150 out of 150 … I used a lot of the Cyber Academy for that paper, like the Fan. And he (student's professor) liked the different approaches I mentioned out of it." While these comments do not profoundly address level 4 of the Kirkpatrick model, they do shed some light on alternative means of evaluating level 4 and in that respect this is an important finding. Perhaps the best comment with respect to overall value came from Student 1 who observed, "Every customer (exposed to these concepts) has told me that if this is how Northrop Grumman thinks, you guys are light years ahead of everybody else". While not a quantitative measure on economic impact, it shows indirect value by customers who are in a position to affect economic decisions.

Fourth, this course advances the state of the practice with respect to both systems thinking and cybersecurity architecture as a science. Developing and enhancing opportunities for systems thinking is fundamental to developing systems engineers in an accelerated fashion [4], [5], [29], [30]. This research showed promise in that respect. Student 6 said "Now that I've taken the class, I can see where it's more of a methodical step by step process in cybersecurity, in securing your data, in developing a framework everything from an operational perspective to perimeter security. It is a science that you need to not just implement but you need to study and hone your skills on a regular basis". On the topic of cybersecurity architecture, Student 6 went on to say " This course brought what I believe to be multiple methodologies and frameworks into one cohesive class. I think it would benefit security engineers and architects to have that comprehensive look on different methodologies and different frameworks. "That last point is also important. The students perceived enough value in the cybersecurity architecture course that all would recommend it to other cybersecurity engineers. Three went on to indicate that the course should be mandatory. From the science and engineering standpoint, Student 7 offered that it "Made it seem more accessible as an engineering discipline". Student 5 indicated "I never really quite thought of it as a science until I took this course and where it shows all the different layers. It puts it more in a logical concept." The research shows that the cybersecurity architecture course is advancing the state of the practice and has some aspects that are worthy of consideration with respect to cybersecurity architecture as a science.

Overall, one of the initial drivers to developing the cybersecurity architecture course solution was to satisfy the shortage of cybersecurity architects [1]. The data shows that this solution is aligned with NICE's goals that call for measures to increase the number of cybersecurity workers, including the population of cybersecurity engineers. The issue of enhancing cyber education and training to produce cybersecurity engineers has been recognized both as a problem and a solution [2], [3]. This research helps to provide a portion of that solution.

6.0 COMMENTS AND BENEFITS

This research provided some candidate criteria for the evaluation of potential and alternative cybersecurity architecture course solutions. Bloom's Taxonomy [6] is an important part of the education construct as it provides the means to assess the level of learning achieved. Relevant and current case studies and exercises [13], [14], [15] are important to reinforce and provide experiential learning. The relevancy and current nature of the case studies implies the exercises should portray successful and recent attacks to maintain context with current threats and current technology [15]. Diagrams and pictorial views are important to visualize the cybersecurity solution and the processes involved in obtaining the cybersecurity solution [31], [32]. The solution also added to the skillset of cybersecurity professionals strengthening their ability to facilitate communication of cybersecurity defence concepts to technical and non-technical audiences.

One key benefit has been that the development of advanced cyber education and training specifically for cyber architecture was shown as key component of constructing repeatable and cost effective cyber solutions. Additionally, operationalization concepts for cyber security architectures were identified. This furthers the ability to develop repeatable processes that in turn develop meaningful cyber security architecture artefacts. And finally, there is a strong inference of a business impact that this architecture helps develop a discriminator in the ability to define a best practice for architecture, enhancing customer confidence.

7.0 REFERENCES

[1] NICE. (2011). National Initiative for Cybersecurity Education Strategic Plan. Retrieved from http://csrc.nist.gov/nice/documents/nicestratplan/Draft_NICE-Strategic-Plan_Aug2011.pdf.

[2] DASDCIIA. (2009). Department of Defence Information Assurance Strategic Plan. Retrieved from http://dodcio.defense.gov/Portals/0/Documents/DoD_IA_Strategic_Plan.pdf.

[3] CNSS. (2008). *2007/2008 CNSS Report: An agenda for safeguarding national security systems*. Retrieved from http://www.cnss.gov/Assets/pdf/CNSS_Report_07-08.pdf.

[4] Davidz, H. (2008). Enabling systems thinking to accelerate the development of senior systems engineers. *Systems Engineering*. Retrieved from http://onlinelibrary.wiley.com/doi/10.1002/sys.20081/abstract.

[5] Davidz, H., Nightingale, D., & Rhodes, D. (2005). Enablers and Barriers to Systems Thinking Development : Results of a Qualitative and Quantitative Study. *Field Studies*. Retrieved from http://www.stevens.edu/ses/cser/2005/authors/35.pdf.

[6] Van Niekerk, J., & Von Solms, R. (2004). Organisational learning models for information security. *The ISSA 2004 Enabling Tomorrow Conference* (Vol. 30). Citeseer. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.106.4619&rep=rep1&type=pdf.

[7] Saydjari, S. (2004) Cyber Defense: Art to Science, *Communications of the ACM, 47*(3), pp. 52-57.

[8] Allen, J. (2005). Information Security as an Institutional Priority. *CERT, Carnegie Mellon University*.

[9] Hamill, J. T., Deckro, R. F., & Kloeber, J. M. (2005). Evaluating information assurance strategies. *Decision Support Systems*, 39(3), 463-484.

[10] Sherwood, J., Clark, A., & Lynas, D. (2005). Enterprise Security Architecture. Computer Security Journal. 21(4). Retrieved from http://www.alctraining.com.au/pdf/SABSA_White_Paper.pdf.

[11] Eloff, J., & Eloff, M. (2005). Information security architecture. *Computer Fraud Security*, 2005(11), 10-16. Elsevier. doi:10.1016/S1361-3723(05)70275-X.

[12] Zachman, J. (1987). A framework for information systems architecture. *IBM Systems Journal*, *26*(3).

[13] Litzinger, T., Lattuca, L., Hadgraft, R., & Newstetter, W. (2011). Engineering Education and the Development of Expertise. *Journal of Engineering Education*, 100(1), 123–150.

[14] Hentea, M., Dhillon, H., & Dhillon, M. (2006). Towards Changes in Information Security Education. *Journal of Information Technology Education*, *5*, 221–223. Retrieved from http://jite.informingscience.org/documents/Vol5/v5p221-233Hentea148.pdf.

[15] Rowe, D., Lunt, B., & Ekstrom, J. (2011). The role of cyber-security in information technology education. *Proceedings of the 2011 conference on Information technology education - SIGITE '11*, *2*, 113 – 121. doi:10.1145/2047594.2047628.

[16] Pereira, C., & Sousa, P. (2004). A Method to Define an Enterprise Architecture using the Zachman Framework. *ACM Symposium on Applied Computing* (pp. 1366–1371).

[17] Sawilla, R. & Wiemer, D. (2011, November). Automated computer network defence technology demonstration project (ARMOUR TDP): Concept of operations, architecture, and integration framework. *In Technologies for Homeland Security (HST), 2011 IEEE International Conference on* (pp. 167-172). IEEE.

[18] Nelson, J., Nelson, D. & Nelson, N. (2009). Information security employment: An empirical study. *Proceedings of the 10th WSEAS International Conference on Mathematics and Computers Business and Economics*, p. 297-300, retrieved on June 11, 2012 from http://www.wseas.us/e-library/conferences/2009/prague/MCBE/MCBE50.pdf.

[19] Jalaliniya, S., & Fakhredin, F. (2011). *Enterprise Architecture & Security Architecture Development. Technology*. Lund University. Retrieved from http://www.enterprisearchitecture.ir/downloads/thesis/Thesis_Shahram%26Farzaneh.pdf.

[20] Osvalds, G. (2011, March). Model-Based Systems Engineering (MBSE) Process Using SysML for Architecture Design, Simulation and Visualization. In *NASA Goddard Space Flight Center Systems Engineering Seminar*.

[21] McCallam, D. (2012, April). *An analysis of cyber reference architectures*. Presented at NATO 2012 Workshop with Industry on Cybersecurity Capabilities, The Hague, Netherlands.

[22] Oh, E., & Park, S. (2009). How are universities involved in blended instruction?. *Educational Technology & Society*, *12*(3), 327-342.

[23] Bayuk, J. (2011). Systems Security Engineering. *IEEE Security and Privacy Magazine*, 9(2), 72–74. doi:10.1109/MSP.2011.41.

[24] Heaney, J., Hybertson, D., Reedy, A., Chapin, S., Bollinger, T., Williams, D., & Kirwan, M. (2002). Information Assurance for Enterprise Engineering. *MITRE Report*, 1–20.

[25] Krefting, L. (1991). Rigor in qualitative research: the assessment of trustworthiness. *The American Journal of Occupational Therapy*, *45*(3), 214–222.

[26] Guba, E. G., & Lincoln, Y. S. (2001). Guidelines and checklist for constructivist (aka fourth generation) evaluation. *Retrieved June*, *18*, 2008.

[27] Rajeev, P., Madan, M., & Jayarajan, K. (2009). Revisiting Kirkpatrick's model – an evaluation of an academic training course. *Current Science*, *96*(2), 272–276.

[28] Alliger, G., Tannenbaum, S., Bennett, W., Traver, H., & Shotland, A. (1998). *A META-ANALYSIS OF THE RELATIONS AMONG TRAINING CRITERIA* (p. 18).

[29] Cabrera, D. (2006). Systems Thinking. (Unpublished doctoral dissertation). Cornell University.

[30] Valerdi, R. & Davidz, H. (2008). Empirical Research in Systems Engineering : Challenges and Opportunities of a New Frontier. *Systems Engineering*, *12*(2), 169–181. doi:10.1002/sys.

[31] Hamilton, J. (2006). DoDAF-Based Information Assurance Architectures. Journal of *Defense Software Engineering*, *February*, 4–7. Retrieved from http://cross5talk2.squarespace.com/storage/issue-archives/2006/200602/200602-Hamilton.pdf.

[32] Amer, S. H., & Hamilton Jr, J. A. (2008, April). Understanding security architecture. In *Proceedings of the 2008 Spring simulation multiconference* (pp. 335-342). Society for Computer Simulation International.

[33] DRDC. (2010). *Statement of Work for the Automated Computer Network Defence (ARMOUR) Technology Demonstration.* Reference document (Version 0.1). Ottawa, ON, CA.