

Effective Belief Network for Cyber Security Frameworks

Issa Atoum¹ and Ahmed Otoom²

¹*Faculty of Information Technology, The World Islamic Sciences & Education
University, 11947 Amman, Jordan*

²*Royal Jordanian Air Forces, 11134 Amman, Jordan*
¹*Issa.Atoum@wise.edu.jo, ²aotoom@rjaf.mil.jo*

Abstract

Cyber security frameworks direct the implementation of cyber security solutions. Managing the implementation of cyber security frameworks is a difficult task due to many problems. Part of these problems are concealed in the framework interdependent components (variables). Various works identified these variables, but they did not show their relationships. In order to reduce potential threats at an early phase of cyber security implementations, a clear understanding of the relationships between these variables is required. This article proposes a causal cyber security belief network in order to facilitate frameworks execution thus reducing threats. The proposed model was tested on random data as well as data provided by the experts. The resultant belief network shows that cyber security objectives are achievable with theoretical minimum threats.

Keywords: *cyber security implementation frameworks, belief networks, cyber security strategy, threat analysis.*

1. Introduction

Implementing cyber security is challenging for every country [1]. It is related to many factors; software, hardware, technology, people and business procedures [2][3]. Cyber security frameworks must provide guidance to management at various security levels before implementation [4]. To help managers, models must be comprehensive and abstract to cover as much as possible of related aspects of cyber security solutions. Atoum *et al.* [4] proposed a holistic cyber security implementation framework in order to holistically resolve management issues.

Figure 1 shows Atoum *et al.* [4] model. The model is holistic (abstractly at the national level). A close look at the figure shows many components: Cyber Security Strategy (CSS) and its goals, the audit and Change Control Board, the business needs, *etc.* Atoum *et al.* [4] showed that the model can basically convert the CSS to goals and then goals can be converted to detailed security requirements. As a result, the requirements is carried out using various security projects. The results of these projects contribute to cyber security goals of the cyber security framework. However, the model does not show how its components are related. Consequently, managing this model (i.e. cyber security model) will need higher management, especially risk and security managers to take care of various aspects at the same time.

Several models were proposed to identify and analyze risks and potential threats of cyber security models [5]–[7]. However, these models are run on real-time or near real-time. Therefore, most security actions are preventive rather than proactive. Henceforward, this article proposes belief networks model in order to help security managers oversee cyber security potential risks at early phase of cyber security execution. Consequently, improving decision making for security investment. The article will be based on the work of Atoum *et al.* [4] because it represents security frameworks holistically. The proposed

model analyses and quantifies information security risks caused by several threat resources.

First, we introduce Bayesian networks. Then, we provide an example on belief networks. Finally, we use belief networks to model cyber security implementation frameworks.

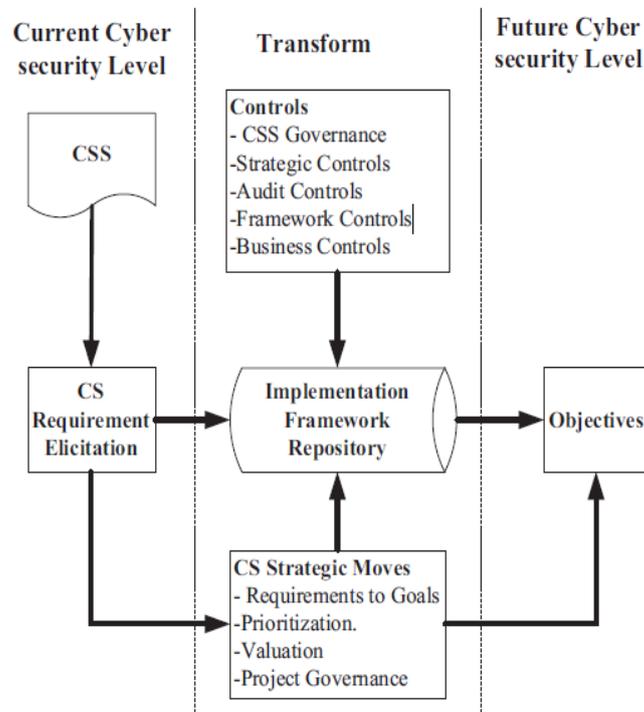


Figure 1. HCS-IF (from Atoum et al. (2012))

2. Bayesian Network Applied to Cyber Security

A Bayesian Network (BN) is a probabilistic graphical model that represents a set of random variables and their conditional dependencies via a Directed Acyclic Graph (DAG) to reason about uncertainty.

The simplest form of the Bayes Theorem (formula (1)):

$$P(A \cap B) = P(A|B)P(B) = P(B|A)P(A), \quad (1)$$

where:

A and **B** are any random events,

$$P(B) \neq 0 .$$

This formula is read as: Probability of A and B = (Probability of A B) TIMES (Probability of B).

The Bayes Chain product rule for **n** variables is defined as in (formula (2)):

(2)

$$P(\bigcap_{k=1}^n A_k) = \prod_{i=1}^n P(A_k | \bigcap_{j=1}^{k-1} A_j),$$

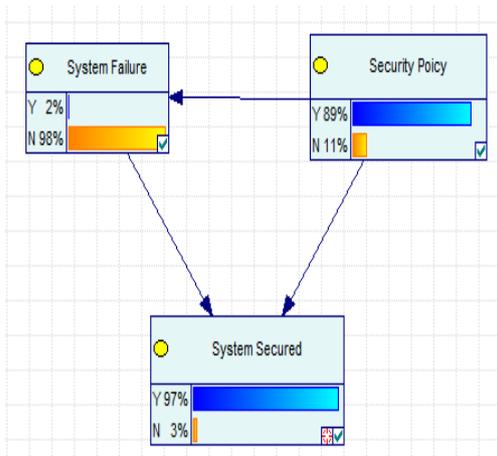


Figure 2. Belief Network Example Before an Evidence is Set

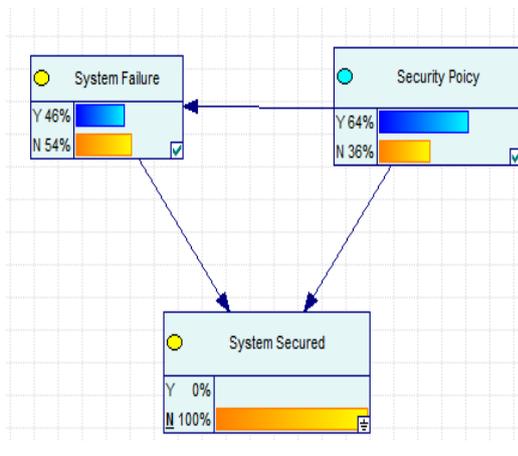


Figure 3. Belief Network Example After an Evidence is Set (S=N)

Table1. Probabilities Values for the BN Example

a.			c.	
System Failure(F)	Security Policy(L)		Security Policy(L)	
	Y	N	Y	N
Y	0.01	0.05	0.9	0.1
N	0.99	0.95		

b.		System Secured(S)	
Security Policy(L)	System Failure(F)	Y	N
Y	Y	0.2	0.8
N	Y	0.1	0.9
Y	N	0.99	0.01
N	N	0.95	0.05

where:

A_k is any random variable k ,

n is number of random variables,

$\bigcap_{k=1}^n A_k$ list of random variables.

To illustrate the BN in an example, suppose that there are two events that could cause a system to be unsecured (S): either the security policy (L) is not enforced or a system failure (F). Also, suppose that the policy has a direct effect on a system being failure. Then the situation can be modelled with a Bayesian Network. All three variables have two possible values, Y (for Yes) and N (for No). See Figure 2, Figure 3 and Table 1.

The model can answer questions like: "What is the probability that a system policy is not enforced, given the system is unsecured?" by using the conditional probability formulas (1), and chain product rule (2):

$$\begin{aligned}
 P(L = N|S = N) &= \frac{P(S = N, L = N)}{P(S = N)} \\
 &= \frac{\sum_{FE\{N,Y\}} P(S=N, L=N, F)}{\sum_{L,FE\{N,Y\}} P(S=N, L, F)} \\
 &= \frac{0.9 * 0.1 * 0.05 + 0.05 * 0.1 * 0.95}{0.9 * 0.1 * 0.05 + 0.05 * 0.1 * 0.95 + 0.01 * 0.9 * 0.99 + 0.8 * 0.9 * 0.01} \\
 &= \frac{0.0045 + 0.00475}{0.0045 + 0.00475 + 0.00891 + 0.0072} \\
 &= \frac{0.00925}{0.00925 + 0.01611} \\
 &\cong 0.36
 \end{aligned}$$

The joint probability will become more difficult to calculate manually especially if the number of variables increases and the number of states increases, so software tools are usually used. Many software tools have set of algorithms that could be used to calculate the probabilities especially for large networks. In this research, we use the GeNIe [8].

3. Related Work

BNs techniques have been applied to various cyber security domains. They are used for intrusion detection systems [9]–[11]. Moreover, BNs is also used for attack graphs at run time [12], [13]. Furthermore, BN has been used to measure and evaluate the security level during system execution [14].

Literature discussed several models to analyze security models by making causal relationships between vulnerabilities and exploits [15]–[17]. Their approaches are based in building attack graphs to show several stages attacks of the enterprise network. [18] proposed a BN model to analyze potential threats of enterprise networks by exploiting data of intrusion response.

To our knowledge there is no work related to cyber security frameworks using belief networks. However, the model of Kondakci [19] could be related to our work. Kondakci proposed a model to assess risk of enterprise networks using BNs. There model is based on pre-calculated probabilities. Most of studied models are based on existing data in real-time however, our approach is at design time.

4. Proposed Model

We use the BN model to formally validate the applicability of the Holistic Cyber Security Implementation Framework of [4] (H-CS-IF). The objective of [4] is to achieve the required security level utilizing a set of controls that have an effect on each other. Figure 4 is the Bayesian belief network model for the HCS-IF using GeNIe software.

In the HCS-IF, the supportive evidence values toward cyber security objectives are mainly: the Controls, the Strategic Moves, the Requirements, Identified Goals and the CSS. Unfortunately, to our knowledge, there is no direct way to calculate the probability of each component. So, we depend on domain knowledge and expert expectation. Furthermore, Trust-Based Security Level Evaluation using Bayesian can be used to integrate both domain expert and knowledge base [14].

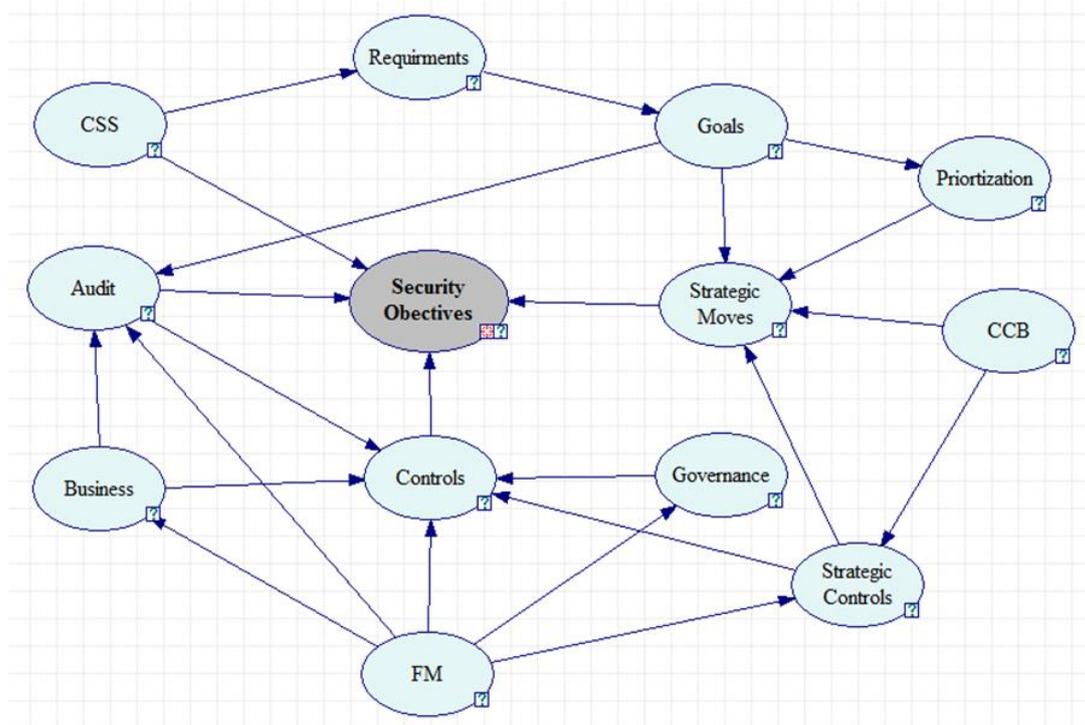


Figure 4. Belief Network of HCS-IF.

Consequently, the proposed BN enables the HCS-IF to lend itself to this suggested validation approach (i.e. BN). The more related components we identify the more accurate the measured security level. As a result, the HCS-IF can give direction in order to guarantee the achievement of the required security level by achieving security objectives.

5. Evaluation

To illustrate the model shown in Figure 4, we make 2 runs, the first with feedback from experts and the result is shown in Figure 5. The latter run is shown in Figure 6 by making evidence that Business, Framework, Audit, Governance, Strategic Controls are not satisfied. We got a security level of 88% in the first case compared to a security level of only 28% in the second case. This results means that the evidence variables have direct effect on the ultimate security level.

A further step has been carried out in order to test the proposed BN; we created 10,000 records of the network with a probability of 50% for each variable. Then, we test the network shown in Figure 6 using the generated data with 10-fold cross validation. The result was 68% for the security objectives success which relatively provides a good indication for the BN model validity.

Unfortunately, we have noticed that the results are highly dependent on the generated data and its distribution. Since we are not able to get data to our model due to fact that most available data sets are on the operational level of cyber security, and even if we were

able to aggregate such data the semantic of the data will get lost. Therefore, the proposed BN is able to give direction to the security managers at early stage of the cyber security implementation.

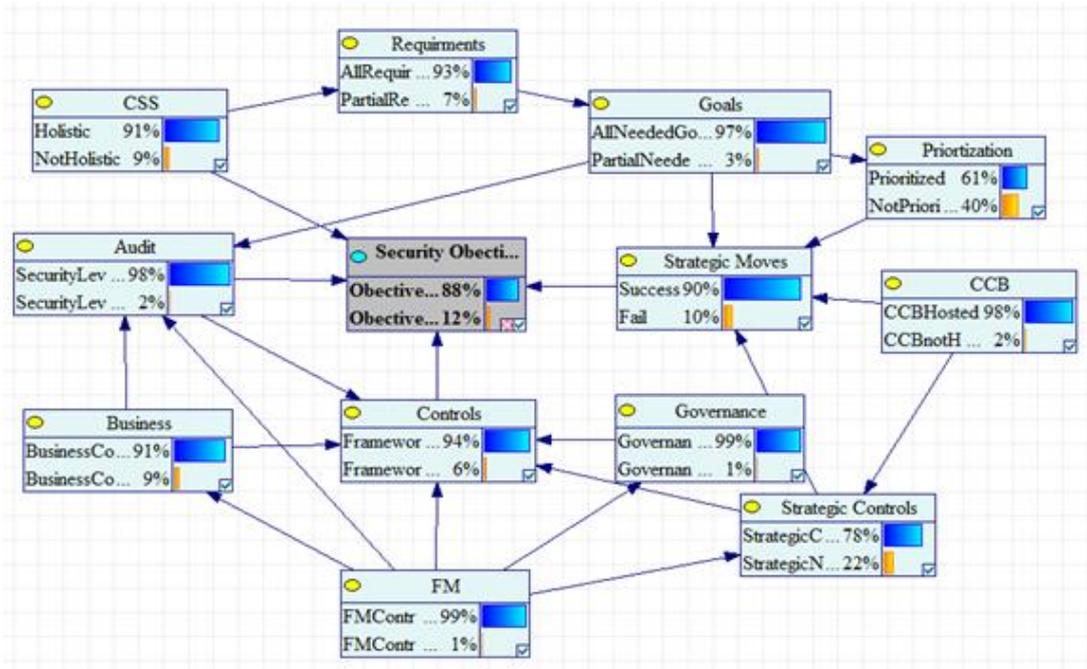


Figure 5. Sample Network of HCS-IF (Assigning Values by Experts)

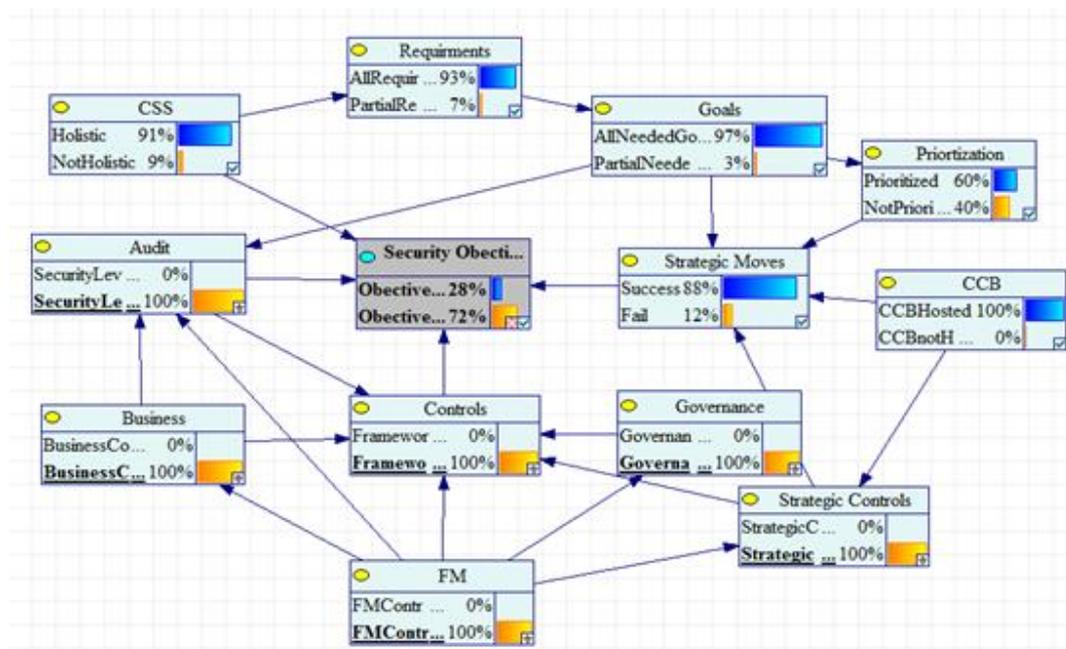


Figure 6. Sample Network of HCS-IF (Assigning Evidence of Controls to False).

6. Conclusion

This article proposed a proactive approach to model cyber security frameworks in terms of its variables. We model a previously proposed cyber security framework using belief networks. The proposed model shows the causal effect between cyber security framework variables, thus it can reduce potential threats at design time. The model was tested on sets of data from experts and random data. Results showed that the proposed model can help understand the relationship between interrelated cyber security variables. It can also give guidance to security engineers and managers.

References

- [1] S. M. Tisdale, "Cybersecurity: challenges from a systems, complexity, knowledge management and business intelligence perspective.," *Issues Inf. Syst.*, vol. 16, no. 3, 2015.
- [2] A. Ootom and I. Atoum, "An Implementation Framework (IF) for the National Information Assurance and Cyber Security Strategy (NIACSS) of Jordan," *Int. Arab J. Inf. Technol.*, vol. 10, no. 4, 2013.
- [3] M. R. Tisdale Susan M., "Cybersecurity: Challenges From A Systems, Complexity, Knowledge Management and Business Intelligence Perspective," *Issues Inf. Syst.*, vol. 10, no. 111, pp. 191–198, 2015.
- [4] I. Atoum, A. A. Ootom, and A. Abu Ali, "A Holistic Cyber Security Implementation Framework," *Int. J. Inf. Secur.*, vol. 22, no. 3, pp. 251–264, 2012.
- [5] S. H. Houmb, I. Ray, and I. Ray, "Trust Establishment in Distributed Networks: Analysis and Modeling," *4th International Conference, iTrust 2006*. Berlin, Heidelberg, Pisa, Italy, May 16-19, 2006. Proceedings, pp. 135–149, 2006.
- [6] Y. L. Sun and Y. Yang, "Trust Establishment in Distributed Networks: Analysis and Modeling," in *Communications, 2007. ICC '07. IEEE International Conference on*, 2007, pp. 1266–1273.
- [7] V. N. L. Franqueira, S. H. Houmb, and M. Daneva, "Using real option thinking to improve decision making in security investment," in *On the Move to Meaningful Internet Systems: OTM 2010*, Springer, 2010, pp. 619–638.
- [8] Decision Systems Laboratory/University of Pittsburgh, "GeNIe & SMILE." University of Pittsburgh, 2011.
- [9] P. G. Bringas, "Intensive Use of Bayesian Belief Networks for the Unified, Flexible and Adaptable Analysis of Misuses and Anomalies in Network Intrusion Detection and Prevention Systems," in *Database and Expert Systems Applications, 2007. DEXA '07. 18th International Workshop on*, 2007, pp. 365–371.
- [10] C. Kruegel, D. Mutz, W. Robertson, and F. Valeur, "Bayesian event classification for intrusion detection," in *Computer Security Applications Conference, 2003. Proceedings. 19th Annual*, 2003, pp. 14–23.
- [11] A. Valdes and K. Skinner, "Adaptive, model-based monitoring for cyber attack detection," in *Recent Advances in Intrusion Detection*, 2000, pp. 80–93.
- [12] M. Frigault and L. Wang, *Measuring network security using bayesian network-based attack graphs*. IEEE, 2008.
- [13] M. Frigault, L. Wang, A. Singhal, and S. Jajodia, "Measuring Network Security Using Dynamic Bayesian Network," in *Proceedings of the 4th ACM Workshop on Quality of Protection*, 2008, pp. 23–30.
- [14] S. Houmb, I. I. Ray, and S. Chakraborty, "Trust-Based Security Level Evaluation Using Bayesian Belief Networks," in *Transactions on Computational Science X*, vol. 6340, M. Gavrilova, C. Tan, and E. Moreno, Eds. Springer Berlin / Heidelberg, 2010, pp. 154–186.
- [15] A. D. Kent, L. M. Liebrock, and J. C. Neil, "Authentication graphs: Analyzing user behavior within an enterprise network," *Comput. Secur.*, vol. 48, pp. 150–166, 2015.
- [16] B. Kordy, L. Piètre-Cambacédès, and P. Schweitzer, "DAG-based attack and defense modeling: Don't miss the forest for the attack trees," *Comput. Sci. Rev.*, vol. 13, pp. 1–38, 2014.
- [17] N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs," *IEEE Trans. Dependable Secur. Comput.*, vol. 9, no. 1, pp. 61–74, Jan. 2012.
- [18] P. Xie, J. H. Li, X. Ou, P. Liu, and R. Levy, "Using Bayesian networks for cyber security analysis," in *Dependable Systems and Networks (DSN), 2010 IEEE/IFIP International Conference on*, 2010, pp. 211–220.
- [19] S. Kondakci, "Network security risk assessment using Bayesian belief networks," in *IEEE International Conference on Social Computing / IEEE International Conference on Privacy, Security, Risk and Trust*, 2010, pp. 952–960.

