Security Risk Learning in Cybersecurity: Evidential Reasoning Model

Authors redacted to preserve anonymity

Abstract:

Information security can only be soundly managed based of security risks to system owners. These risks can only be managed if there is an effective process in place to learn risks and plan incident responses accordingly. Such a cybersecurity environment is however full of uncertainties and ambiguities beyond what Bayesian theory can handle. Hence, an evidential reasoning strategy using Dempster and Shafer Theory becomes essential in learning those security risks for planning a business continuity management system and for handling real-time incident responses. We propose an evidential reasoning model that can learn risks based the AIC triad model – availability, integrity, and confidentiality – and express those security risks as the plausibility of failing to assure them. Available evidence throughout the cybersecurity environment is partitioned accordingly and a sequential belief structure is processed to lead to a comprehensive assertion based on which the security risk to owners is expressed. A numerical example is provided to demonstrate the working of the proposed model.

Keywords: cybersecurity, evidential reasoning, security risk, Dempster and Shafer Theory, availability, data integrity, confidentiality.

The risk management life cycle

Security risk management, as shown in Figure 1, consists of set of recurrent and documented phases: risk planning, risk analysis, risk treatment, and risk monitoring. This is also referred to as the risk management life cycle [1]. Risk management is the activity of controlling risk to maintain it within an acceptable range. It includes planning for risk, assessing risk areas, developing risk-treatment options, monitoring risks to determine how risks change, and documenting the overall risk management program. Risk planning is the process of developing and documenting an organized, comprehensive, and interactive strategy and methods for identifying and tracking risk areas, developing risk treatment plans, performing continuous risk assessments to determine how risks change, and assigning adequate resources. Risk assessment is the determination of the level of risk and the potential impact of identified risk by measuring the likelihood and the impact if associated incidents would take place. Risk assessment is needed to prioritize any risk treatment effort devised to protect the system in question. The amount of risk assessed will be compared against expected benefits before any risk treatment is approved.

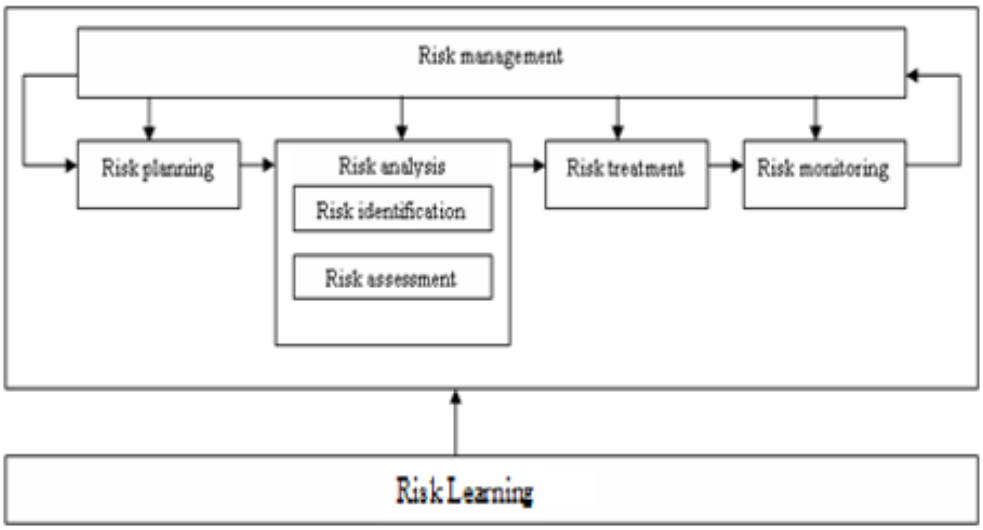


Figure 1: Risk management lifecycle, adapted from the U.S. Department of Energy.

Risk analysis is the process of examining each identified risk area or process to refine the description of the risk, isolating the causes, and determining the effects. It includes risk rating and prioritization in which risk events are defined in terms of their probability of occurrence, severity of consequence/impact, and relationship to other risk areas or processes. Risk treatment is the process of defining, selecting, and implementing security controls in order to bring back risks to acceptable levels as defined in security policy. This includes the terms of what should be done, when it should be accomplished, who is responsible, the schedule, and relevant costs. Risk monitoring is the process that systematically tracks and evaluates the performance of risk treatment actions against established metrics and develops further risk treatment options, as needed. This process revisits back to the other risk management activities of planning, analysis, and treatment as shown in Figure 1. This represents the cycle in the risk management process. Lastly, risk learning is the capturing of any available evidence on the behavior of the cybersecurity environment that effects available information on security risks.

Assets may be exposed to a chance of 'loss;' that is, loss of availability, confidentiality, or integrity. If the asset is exposed to a chance of loss of this type, then the owner is exposed to a chance other types of loss: loss of business and loss of non-economic benefits (or social benefits). The loss of confidentiality, integrity, or availability of an asset will translate into loss of business value to the organization [1]. The organization will also lose its reputation, the trust of its partners and customers, in addition to many other undesirable social outcomes. If the loss is realized, because of an undesired even that we failed to prevent from occurring, then the organization will lose all the revenues generated by the normal operations of the victim asset throughout the asset recovery period, in addition to social benefits. Unless those undesired events are prevented and asset vulnerabilities are mitigated there is always a chance that losses would take place.

Evidential model for learning security risks

Information security management of a system is the assurance that its total security risk remains continuously within the security risk range imposed by its own security policy. Let us write overall system security risk R_s in terms of all effecting factors. In general, one can always think of a set of major components C_i, i=1,N for which we can assess risks R_i, i=1,N. The overall system security R_s can then be written in terms of the risks R_i, i=1,N. These latter risks can in their turn be expressed in terms of all known assets' vulnerabilities $E_3=\{\{E_{11}, \ldots, E_{1M1}\}, \ldots, \{E_{1M}, \ldots, E_{1MM}\}\}$, as shown in Figure 2. The

evidence processing mechanism will first produce the components' assertions $\{a_1, \ldots, a_N\}$ based on evidence E_3 on assets' vulnerabilities and existing threats then the main assertion a_s in terms of components assertions $\{a_1, \ldots, a_N\}$ and available evidence on the current information security management process E_0.

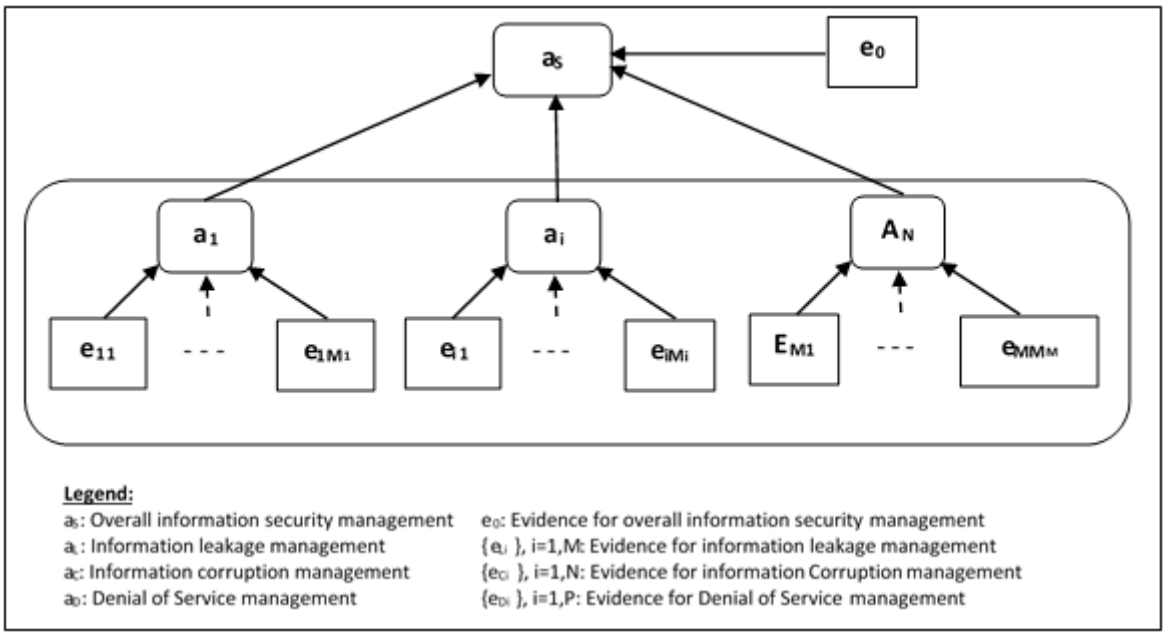


Figure 2: General evidence structure for risk learning

The security policy of a system defines both its real-time and its general acceptable computing behavior, as defined by its owners [1]. In this article, we are only concerned with three classes of security disruptions, as in Raggad taxonomy [1]: information leakage, information corruption, and denial of service.

We assume the information security manger conducts it security management role based on 4 information security resources: E_L: evidence related to information leakage, E_C: evidence related to information corruption, E_D: evidence related to denial of service, and E_0: evidence related to the independent activity of managing the system according to system security policy.

The resources of evidence E_L, E_C, and E_D collect their own evidences from their own sources: E_L acquires its own evidence from M sources $\{E_{Li}\}$, i=1,M; E_C acquires its own evidence from N sources $\{E_{Ci}\}$, i=1,N; and E_D acquires its own evidence from P sources $\{E_{Ci}\}$, i=1,N;. The independent resource of evidence E_0 is articulated by information security management based on what they know they are doing to protect their computing environment according to their owners' security policy. Figure 1 depicts the evidence structure just discussed above and processed for the purpose of learning the system security risk in a continual manner.

The overall security risk of the computing environment R_s is computed in terms of the individual risks R_L, R_C, and R_d, and R_0 representing respectively system risk of information leakage, system risk of information corruption, denial of service risk, and ineffective system security management risk. While we are processing the evidential scheme above, there are many quantities of interest that propagate from the higher nodes of evidence at the leaves of the tree, to lower layers representing the individual information security risks, until the main assertion defining the overall information security management root where the overall system security risk is evaluated, as depicted in Figure 3.

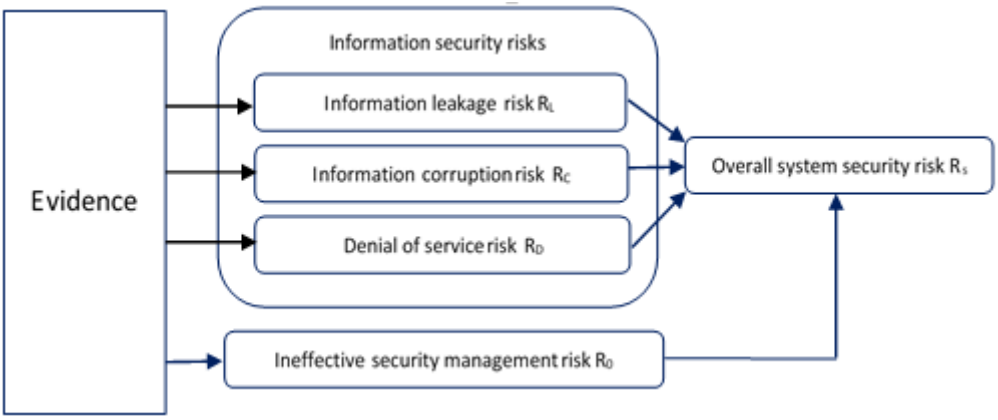


Figure 3: Limited Structure for learning risks based on the AIC triad.

Evidential reasoning

Belief functions, used in this article to construct our evidential reasoning model, were introduced in the 70's under a more extended framework called Dempster and Shafer Theory (DST) [3]. In the situations of poor or incomplete data, uncertainty management in Dempster and Shafer took a more intuitive approach and deviated from the conventional formalism adopted in Bayesian theory. In a DST setting, we start with the delineation of propositional space called a frame of discernment that contains all possible states, in an exhaustive and mutually exclusive way, so that only one of them can take place in one given time. Let us denote this space as $\Omega=\{w_i\}_{i=1,|\Omega|}$ where w_i, i=1,|Ω| denotes a possible state of the our frame of discernment Ω.

Uncertainties are represented through a basic belief assignment that produces the m-values given the information on hand [4]. The m-values are only assigned to subsets of the elements for which we have information. We then have:

$m: 2^{\Omega} \rightarrow [0\ 1]$
$Bel(A) = \sum X \in A\ m(X)$ for any A in 2^{Ω}

The plausibility function on a sunset A is defined as the degree to which A is plausible in light of the evidence, or alternatively, the degree to which A is not disbelieved [6]. The evidential security management risk scheme may be presented using the belief structures used to capture the individual information security risks and the security management risk that we combined to produce the overall system security risk R_s [2, 4]:

E_L= {
$m_L: 2^{\Omega L} \rightarrow [0\ 1]$;
Ω_L= {w^+_L='adequate information leakage management',
w^-_L='inadequate information leakage management'};
$e_L = (e^+_L = m_L(w^+_L); e^-_L = m_L(w^-_L); m_L(\Omega_L) = 1 - e^+_L - e^-_L)$
}

E_C= {
$m_C: 2^{\Omega C} \rightarrow [0\ 1]$;
Ω_C= {w^+_C='adequate information corruption management',
w^-_C='inadequate information corruption management'};

e_C = (e^+_C=m_L(w^+_C); e^-_C=m_C(w^-_C); m_C(Ω_C)=1 - e^+_C - e^-_C)
}

E_D= {
m_D: $2^{\Omega D}$ →[0 1];
Ω_D= {w^+_D='adequate denial of service management',
w^-_D=' 'inadequate denial of service management'};
e_D = (e^+_D=m_L(w^+_D); e^-_D=m_D(w^-_D); m_D(Ω_D)=1 - e^+_D - e^-_D)
}

E_0= {
m_0: $2^{\Omega 0}$ →[0 1];
Ω_0= {w^+_0='adequate overall system security management',
w^-_0=' 'inadequate overall system security management'};
e_0 = (e^+_0=m_L(w^+_0); e^-_0=m_0(w^-_0); m_0(Ω_0)=1 - e^+_0 - e^-_0)
}

E_s= {
m_s: $2^{\Omega L}$ →[0 1];
Ω_s= {w^+_s='adequate system security', w^-_s=' 'inadequate system security'};
e_s = (e^+_s=m_s(w^+_s); e^-_s=m_s(w^-_s); m_s(Ω_s)=1 - e^+_s - e^-_s)
}

The evidence propagation process

According to the AIC triad model for availability, integrity and confidentiality, we know that any security disruption encountered in a computing environment will add risk to one of these menaces, respectively associated with denial of service, information corruption, and information leakage. That is, all evidence accumulated on information security risks will lead to a revision of all their belief structures that are processed to produce main (lower level in the evidential hierarchy) assertions on the hierarchic evidence scheme discussed above. The propagation of the processed evidence is computed as shown in Figure 4. As an example, suppose we have two pieces of evidence on the risk of information leakage:

E_L={$e_{L1}$and e_{L2}}
{m_{L1}: $2^{\Omega L1}$ →[0 1];
Ω_{L1}= {w^+_{L1}='adequate information leakage software',
w^-_{L1}='inadequate information leakage software'};
e_{L1} = (e^+_{L1}=m_{L1}(w^+_{L1}); e^-_{L1}=m_{L1}(w^-_{L1}); m_{L1}(Ω_{L1})=1 - e^+_{L1} - e^-_{L1}).}

{m_{L2}: $2^{\Omega L2}$ →[0 1];
Ω_{L2}= {w^+_{L2}='adequate budget for information leakage management',
w^-_{L2}='inadequate budget for information leakage management'};
e_{L2} = (e^+_{L2}=m_{L2}(w^+_{L2}); e^-_{L2}=m_{L2}(w^-_{L2}); m_{L2}(Ω_{L2})=1 - e^+_{L2} - e^-_{L2}).}

These are two independent sources of evidence that we can combine to produce the belief structure of the assertion on information leakage management, as follows:

{m_L: $2^{\Omega L}$ →[0 1];
Ω_L= {w^+_L='adequate information leakage management',
w^-_L='inadequate information leakage management'};
$m_L(w^+_L)$ =[m_{L1}(w^+_{L1}) m_{L2}(w^+_{L2}) + m_{L1}(w^+_{L1}) m_{L2}({w^+_{L1}, w^-_{L1}}) + m_{L1}({w^+_{L1}, w^-_{L1}})m_{L2}(w^+_{L2})]/(1-k_L)
$m_L(w^-_L)$ = [m_{L1}(w^-_{L1}) m_{L2}(w^-_{L2}) + m_{L1}(w^-_{L1}) m_{L2}({w^+_{L1}, w^-_{L1}}) + m_{L1}({w^+_{L1}, w^-_{L1}})m_{L2}(w^-_{L2})]/(1-k_L)
Where: k_L= m_{L1}(w^+_{L1}) m_{L2}(w^-_{L2}) + m_{L1}(w^-_{L1}) m_{L2}(w^+_{L2})}

We start learning system security risks as early as at the leaves of evidence at the highest level of the hierarchic evidence scheme. The original sources of risks are found at asset vulnerabilities, as shown in Figure 3. The ability of the existing threats to exploit these vulnerabilities will shape the amounts of risks. Risk develops when we become capable of acquiring information on how current threats exploits asset vulnerabilities and the impact on the business value an asset can generate. In this example, there are plenty of threats that can produce information leakage, and plenty of threats that will produce information corruption, and also plenty will produce denials of service.

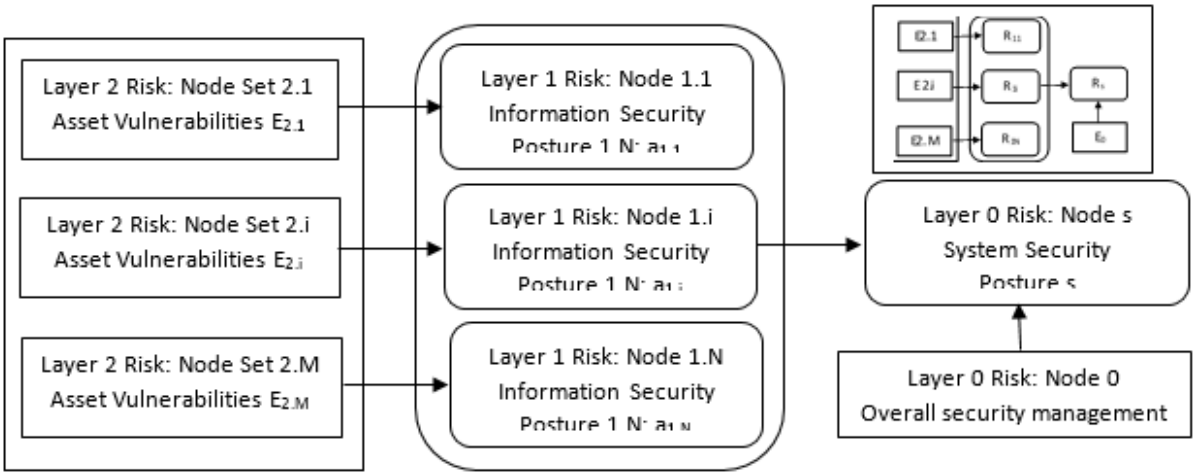
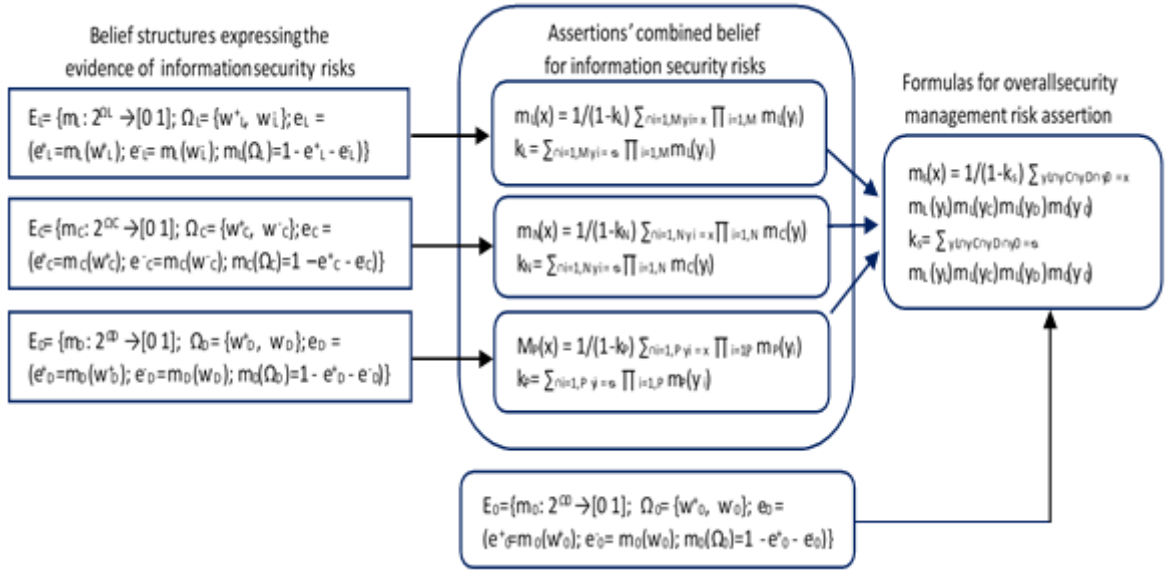


Figure 4: Risk evidential scheme.

That is, there are three subsets of evidence E_L for information leakage, E_C for information corruption, and E_D for denial of service that are available to the respective information security managers to process and produce information on the state of information security in their departments. The information leakage manager will process the evidence subset at hand E_L to produce the assertion a_L. At the same time, the information corruption manager will process all the evidence E_C at hand and produce his/her assertion a_C on the state of information corruption management. On the other hand, the denial of service manager will process all the evidence E_D at hand and produce his/her assertion a_D on the state of denial of service management.



Fog 5. Evidence belief structure expressing overall security management.

Numerical Example

In this numerical example, we assume that we obtained factual evidence as belief structures on the management of information confidentiality, personal training programs, data integrity management, the enforcement of security policy, security planning, and security auditing, as follows:

E_L= {
{m_{L1}: $2^{\Omega L1}$ →[0 1]; Ω_{L1}= {w^+_{L1}: 'Adequate Management of Information Confidentiality', w^-_{L1}: 'Inadequate Management of Information Confidentiality'}; e_{L1} = (e^+_{L1}=.6; e^-_{L1}= .3; $m_{L1}(\Omega_{L1})$=.1)}

{m_{L2}: $2^{\Omega L2}$ →[0 1]; Ω_{L2}= {w^+_{L2}: 'Adequate Personnel Training Programs', w^-_{L2}: 'Inadequate Personnel Training Programs'}; e_{L2} = (e^+_{L2}=.7; e^-_{L2}= .2; $m_{L2}(\Omega_{L2})$=.1)}
}

E_C= {
{m_{C1}: $2^{\Omega C1}$ →[0 1]; Ω_{C1}= {w^+_{C1}: 'Adequate Management of Data Integrity', w^-_{C1}: 'Inadequate Management of Data Integrity'}; e_{C1} = (e^+_{C1}=.6; e^-_{C1}= .1; $m_{C1}(\Omega_{C1})$=.3)}

{m_{C2}: $2^{\Omega C2}$ →[0 1]; Ω_{C2}= {w^+_{C2}: 'Adequate Enforcement of Security Policy', w^-_{C2}: 'Inadequate Enforcement of Security Policy'}; e_{C2} = (e^+_{C2}=.5; e^-_{C2}= .1; $m_{C2}(\Omega_{C2})$=.4)}
}

E_D= {
{m_{D1}: $2^{\Omega D1}$ →[0 1]; Ω_{D1}= {w^+_{D1}: 'Adequate Security Planning', w^-_{D1}: 'Inadequate Security Planning'}; e_{D1} = (e^+_{D1}=.4; e^-_{D1}= .3; $m_{D1}(\Omega_{D1})$=.3)}

{m_{D2}: $2^{\Omega D2}$ →[0 1]; Ω_{D2}= {w^+_{D2}: 'Adequate Security Auditing', w^-_{D2}: 'Inadequate Security Auditing'}; e_{D2} = (e^+_{D2}=.5; e^-_{D2}= .3; $m_{D2}(\Omega_{D2})$=.2)}
}

These subsets of evidence, as depicted in Figure 5, are related to the assertions of information security management in terms of information leakage management, information corruption management, and denial of service management. The evidential propagation process is shown in Figure 6 which produced a security risk of 0.031. Computations may be requested through email from one of the authors of the article.

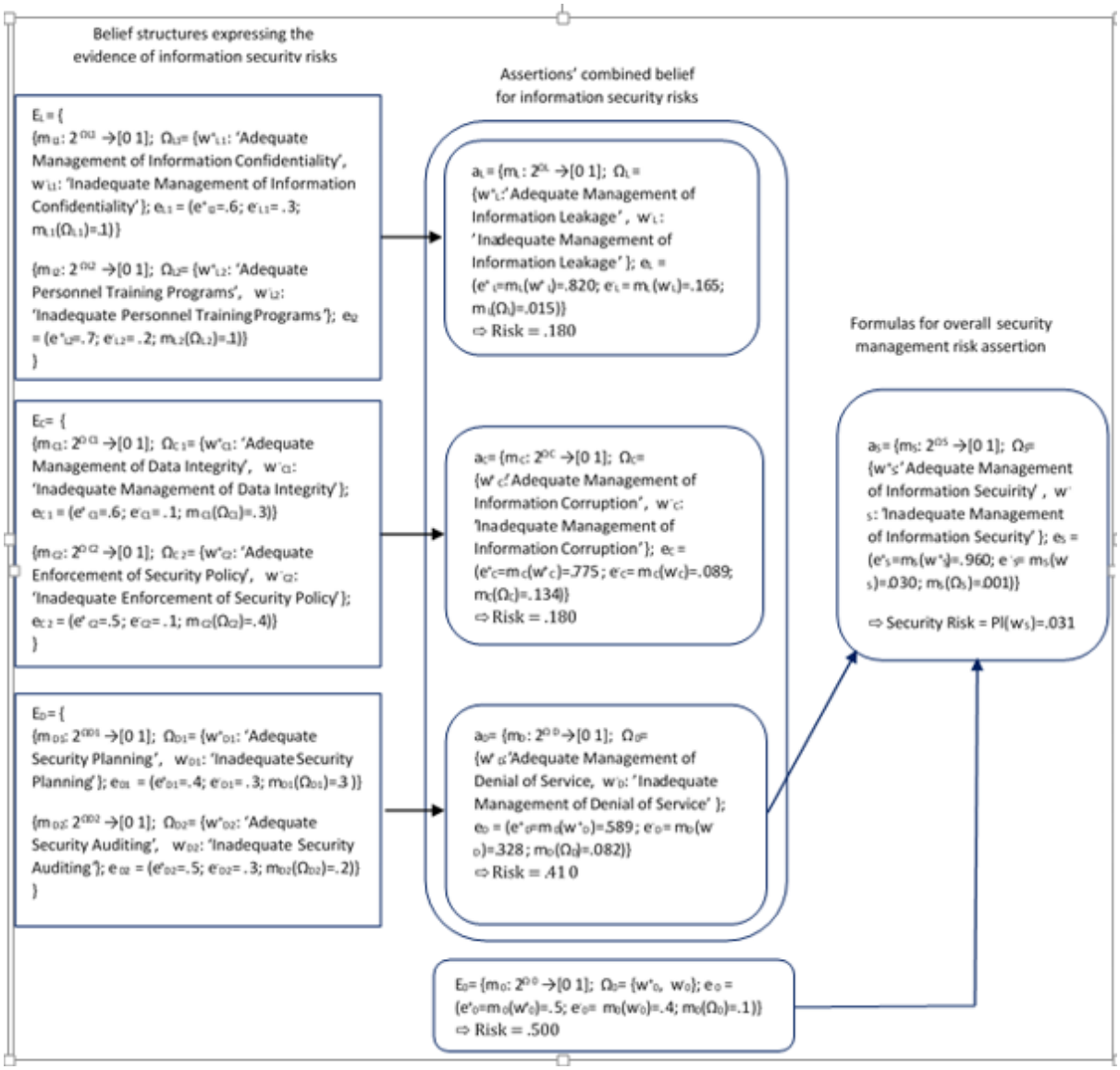


Figure 6: Numerical example to demonstrate the risk learning model.

Conclusion

This article proposed a security risk learning model using evidential reasoning that tracked risks using three layers of risk management. The first layer aimed at capturing evidence at the vulnerability level. The captured vulnerably evidence subsets were processed to produce belief structures on information security management assertions processed at the second layer. The third layer was concerned with the computation of the overall security risk in terms of individual risks associated with information leakage management, information corruption management, and denial of service management. A numerical example, Figure 6, was processed to demonstrate the working of our security risk learning model.

References

1. Raggad, B., Information Security Management, CRC Press, New York, 2010.
2. Shafer, G., A Mathematical Theory of Evidence, Princeton University Press, 1976.

3. Shafer, G. and R. Srivastava, “The Bayesian and Belief-Function Formalisms: A General Perspective for Auditing,” Auditing: A Journal of Practice & Theory, Vol. 9 Supplement, pp 110-137, 1990.
4. Smets, P. The Combination of evidence in the transferable belief model. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 12(5), pp 447-458, 1990.
5. Srivastava, R. P., and Mock, T. Why we should consider belief functions in auditing research and practice. *The Auditor's Report*, 28(2), pp 58-65, 2005.
6. Srivastava, R. P.,and Liu, L. Applications of belief functions in business decisions: A review. *Information Systems Frontiers* 5(4), pp 359-378, *2003.*