

## Cost effective management frameworks for intrusion detection systems

Charles Iheagwara<sup>a</sup>, Andrew Blyth<sup>b</sup> and Mukesh Singhal<sup>c</sup>

<sup>a</sup> *Una Telecom, Inc., 4640 Forbes Boulevard, #200, Lanham, MD 20706, USA*

<sup>b</sup> *School of Computing, University of Glamorgan, Pontypridd, Wales, CF 37 1DL, UK*

<sup>c</sup> *Department of Computer Science, The University of Kentucky, 773 Anderson Hall, Lexington, KY 40506, USA*

This paper discusses the financial benefit of intrusion detection systems (IDS) deployment techniques and addresses the problems of bridging the gap between technical security solutions and the business need for it. This is an area of interest to both the research and the business community; most IDSes balance host and network monitoring, but the decision about how to adjust usage of each technique tends to be made in a rather ad-hoc way, or based upon effectiveness of detection only without regard to cost of technique. In practice, selections based on how well a strategy helps a company to perform are preferable and methodologies supporting a selection process of this type will assist an Information Technology officer to explain security mechanism selections more effectively to CEOs. In this context, the approach we propose could be applied when choosing one intrusion detection system over another based on which has a better or higher return on investment for the company.

Through a case study, we illustrate the benefits of a better IDS management that leads to a positive Return on Investment (ROI) for IDS deployment. We conceive strategies and approaches to support effective decision-making about which techniques are appropriate for the cost effective management of the IDS in a given environment. It is our intent that this research will serve as a foundation for the formal description of cost structures, analysis, and selection of effective implementation approaches to support the management of IDS deployments.

### 1. Introduction

Independent of implementation costs, the method in which security devices such as IDSes are managed can have a serious effect on the Return on Investment (ROI). Thus, a positive ROI for the IDS is dependent upon an organization's deployment strategy and how well the successful implementation and management of the technology helps the organization achieve the tactical and strategic objectives it has established.

However, given the high cost of IDS deployments especially when multiple deployments are involved, organizations must justify implementation expenses by proving that the IDS is a value added resource. One possible justification is to establish that the deployment of the IDS should lead to a reduction in the annual loss expectancy (ALE) and the return on security investment (ROSI).

One method for justifying IDS is by determining the value of the ALE using conventional cost/benefit (risk) assessment; the ALE represents the cost/benefit break-even point for risk mitigation measures. In other words, the organization could justify spending up to the dollar amount equivalent of the ALE per year to prevent the occurrence of loss or reduce the impact of a cyber attack for example. An alternative method for justifying IDS is to demonstrate the ability of the IDS to effectively detect and deter attacks in cost-effective quantifiable measures or to implement it as a standard due care measure. There are prior research studies [1–3] on this. Another option is to analyze the benefits of IDS by documenting the misuses of an organization's network

Hence, for many organizations, investment decisions on IDS deployment will hinge on the ability to demonstrate a positive ROI and are not just motivated by the needs of security risk management. For the IDS to be cost-effective, it should cost no more than the expected level of loss from intrusions. This requires that the IDS purchaser consider the trade-off among cost factors [4,5], which at the minimum should include the cost of damage or compromised asset due to an intrusion, the cost of manual or automatic response to an intrusion, and the operational cost, which measures constraints on time and computing resources. For example, an intrusion where the response or mitigation cost is higher than the damage cost should usually not be acted upon beyond simple logging.

Therefore, implementation costs are very important and should be among the determinant factors for effective IDS management. Although in current IDS implementations, cost value propositions are rare due to the complexities of the networked environment in which they are deployed. Another reason for this is the fact that many organizations are not educated about the cost-benefits of security systems and for some, analyzing site-specific cost factors could be very challenging [6].

The challenge could be partly attributed to the difficulties in the assessment of costs related to computer security, in part because accurate metrics have been inherently unrealistic. Of those costs that can be measured, the largest in terms of monetary value typically involve theft of proprietary information or financial fraud. Others that are more difficult to quantify but have resulted in severe loss of use or productivity include viruses and malware, Web server denial-of-service attacks, abuse of access privileges, and equipment vandalism or outright theft. The challenge is also due to the fact that cost structures and cost management (and costing for that matter) of IT security devices have not been extensively studied; at least not very well documented in technical or scientific literature. The few available studies have been presented from different perspectives.

In the business arena, management costs are calculated through cost benefit analysis (CBA) models/equations with a high degree of accuracy. Here, the models incorporate the use of risk-adjusted cash flows in order to examine internal rate of return (IRR) and maximum net present value (NPV) figured as a percentage of information security expenditures. The basis for this is the observation that a simple return on investment (ROI) calculation that divides income by asset value is insufficient because

it is based on historical rather than future valuations as affected by breach incidents. A more elaborate discussion of CBA is given in Section 2.

The increase in the use of IDS products mandates formulation of appropriate frameworks for their cost-effective management. Such frameworks among others could be used to translate existing cost models into technical solutions as implementation cost structures. This could be realized by first developing the cost metrics and then integrating them with existing theoretical cost models developed in previous studies within the contexts of the frameworks we propose in this research.

The insights gained from previous research studies that describe proven techniques to implement the technologies could be helpful in understanding effective management techniques for IDS deployments. Research in the area of cost modeling for network intrusion detection systems typically follow a risk analysis procedure to select sensitive data/assets and create a cost matrix for each intrusion.

Wei et al. [7] propose a cost-benefit analysis methodology and build a cost model that can be used to quantitatively and qualitatively calculate the cost of detecting and responding to an intrusion.

Lee [4] and Stolfo's [5] studies the problem of building cost-sensitive intrusion detection models and define cost models to formulate the total expected cost of IDS and examine the major cost factors associated with IDS, which include development cost, operational cost, damage cost due to successful intrusions, and the cost of manual and automated response to intrusions. The cost components related to intrusion detection are:

- Damage cost;
- Operation cost; and
- Response cost.

Combining the above cost components Lee [4] proposes a cost matrix for a risk analysis calculation:

$$\text{Cost\_total}(e) = \sum_{i=1}^N (\text{CCost} + \text{OperationCost}(e)). \quad (1)$$

In the above formula, Cost total( $e$ ) is the total cost for some event  $e$ ,  $N$  is the event number, and CCost is the consequential cost of the prediction by the network intrusion detection system for the intrusion event  $e$ , which is determined by the damage cost and response cost. The Damage cost (DamageCost) represents the maximum amount of damage to an attack target when the intrusion detection system and other protective measures are either unavailable or ineffective. The Response cost (ResponseCost) is the cost of responding to the intrusion, which includes taking some action to stop the intrusion and reduce the damage. These actions or countermeasures should be defined during the risk analysis process according to specific threats. Operation cost (OperationCost) is the cost of processing the stream of events being monitored by an intrusion detection system and analyzing the activities using intrusion detection models.

Table 1  
Security cost examples

Security service	Service area	Mechanism	Cost measure
Data confidentiality	NC	Link layer 40-bit DES	Processor clocks per byte
Message non-repudiation	ES	Remote non-repudiation service	$2n$ bytes per message network bandwidth, plus $c$ clocks per byte
Intrusion detection	TS	Experimental system	$N$ Mbytes per second of overall bandwidth, plus $m$ instructions per second, plus $b$ bytes per second storage

Thus, Lee's [4] major contribution to IDS cost models is that he proposed a cost matrix that combines the different cost features defined above for a risk analysis calculation.

For intrusion detection, Irvine [8] defines auditing of network control functions in intermediate nodes, and rule-based network intrusion systems in the total subnet as the mechanisms. Irvine also discusses the costs of those security services and mechanisms (Table 1).

In Irvin's proposition, security services include data confidentiality, integrity, traffic flow confidentiality, authenticity, non-repudiation, availability, audit and intrusion detection, and boundary control. For the three service areas delineated for security service analysis, a client or server system is an example of ES, routers and switches are the examples of IN, and NC indicates the wires that connect systems and nodes. Additionally, Irvin defines Total Subnet (TS) as a service area that can't be assigned exclusively to IN, NC or ES and defines at least one security mechanism for each security service and service area. For example, to protect data confidentiality, he defines operating system and cryptographic credentials as the security mechanism in the ES and IN's. Irvine also defines auditing of network control functions in IN and rule-based network intrusion systems in TS as the mechanisms.

The above propositions are difficult to realize because the units of the cost measure are impracticable to use. Equally, the lack of a quantitative and qualitative cost-benefit analysis and cost benefit tradeoff criteria for the computer security services complicates the application of the proposition.

In another cost model [9], five different prediction cases are identified as False Negative (FN), True Positive (TP), False Positive (FP), True Negative (TN) and Misclassified Hit.

False Negative (FN) is the cost of not detecting an attack. FN is incurred either by a system that does not install an intrusion detection system, or one in which the intrusion detection system does not function properly and mistakenly ignores an attack. This means that the attack will succeed and the target resource will be damaged. The FN cost is therefore defined as the damage cost of the attack. True Positive (TP) occurs in the event of a correctly classified attack, and involves the

cost of detecting the attack and responding to it. This is represented by the formula “Progress  $\times$  DamageCost”, where Progress is the percent of the attack’s progress.

False Positive (FP) occurs when an event is incorrectly classified as an attack. True Negative (TN) cost is always 0, as it is incurred when a network intrusion detection system correctly decides that an event is normal. Misclassified Hit cost is incurred when the wrong type of attack is identified. If the response cost is less than the damage cost, a response action will be taken to stop the attack. Since the action is not useful for the actual attack, some damage cost occurs due to the progression of the true attack.

The above cost model [9] may be impracticable to use and it is not clear how to account the cost for management, maintenance, etc.

In contrast to the above, our contribution in this study is to use reverse engineering technique to formulate appropriate cost-effective management frameworks for IDS implementations. Using the knowledge and experiences gained in the implementation of IDSes, we demonstrate how different management techniques affect the return on investment and will then craft the frameworks around these experiences to improve operational and implementation costs. The frameworks we propose are effective in assessing network intrusion detection systems. They can be used to periodically review the effectiveness of planned and implemented IDSes to determine if they are doing what they are supposed to do, rather than add more cost than the anticipated benefit.

The rest of the paper is organized as follows. In Section 2, we review the state-of-the-art of cost benefit analysis techniques that have been proposed by other researchers. Implementation approaches are discussed in Section 3 and management and costs structures are presented in Section 4. In Section 5 we present a case study that explores the effects of different implementation schemes on the return on investments. We then propose effective management frameworks in Section 6 and conclude our discussion in Section 7.

## 2. The state-of-the-art of cost benefit analysis techniques

One of the most important problems facing information assurance is coming up with a method that accurately calculates the costs associated with lost. This in part is because accurate metrics have been inherently unrealistic. Of those costs that can be measured, the largest in terms of monetary value typically involve theft of proprietary information or financial fraud. Others that are more difficult to quantify but have resulted in severe loss of use or productivity include viruses and malware, Web server denial-of-service attacks, abuse of access privileges, and equipment vandalism or outright theft. Results of surveys of organizations provide estimates as to breach incidents, security expenditures, malicious code, and so on, with numbers continuing to reflect dramatic growth each year. However, lacking any way to translate such statistics into expenditures and losses per organization, per computer, or per user, the

true impact of these figures remains uncertain. An alternative method has been to use the Annual Loss Expectancy (ALE) to estimate risks and hence project potential losses that could result from the risks materializing.

The ALE, a quantitative method for performing risk analysis has been used as one of the earliest estimators in the computer industry was. The ALE is used to calculate risk estimates by multiplying the estimated frequency of occurrence of attacks by the possible loss amount for each data file, and then summing these results. The method has been criticized because of the “lack of empirical data on frequency of occurrence of impacts and the related consequences” thus producing an interpretation of “results as having more precision than they actually had” [10]. Nevertheless, the ALE figures may still provide some useful information. As a result, information technology companies are now resorting to using the established Cost-Benefit Analysis (CBA) method.

The CBA, which has become the most popular metrics, is applied to the assessment of computer-related risks. CBA is well established in microeconomic and management accounting theory, and can be used to determine estimated levels of expenditures appropriate to the values of assets requiring protection. Hazlewood [11] contends that it is particularly convincing since “most managers and directors know little about computers and computer security, but they do understand risk and cost-benefit analysis”. The National Institutes of Health (NIH) has a useful guidance document for preparing CBAs as required by the US. Federal government to support IT management decisions [12]. Although the NIH document does not specifically pertain to security, many of the IT topics and examples discussed are highly relevant, so it is worth a close look.

CBA concepts are distinctively multiple depending on the manner and environment of their application. In IT fields, CBA models are increasingly becoming important in cost estimations and have been effective in assessing network intrusion detection systems. The process involves first performing a risk analysis that produces a cost matrix for the assets under attack, and then independently calculating damage, response, and operation costs for those assets. Resources to counter the attack can be classified as low, medium, or high, in terms of price, and weighted by amounts of use where appropriate, to obtain total expenditures. Probabilistic models also include false negative and false positive costs, since these may have an impact on losses.

An example of early CBA use in computer security is in the I-CAMP (Incident Cost Analysis Modeling Project) model developed by the Big Ten Universities during the 1990s. Factored together are the time, wages, overhead, and direct costs related to the resolution of individual security incidents. Person-hours are logged, typically for incident investigation, system administration, and recovery efforts and then salary-weighted sums (including benefits) are computed. Necessary direct expenditures (such as for replacement hardware, software, and analysis tools) are also added. The I-CAMP model is appropriate for situations where the related usage losses are considered to be modest or ignored entirely.

There are other costs that may be incurred with security protection mechanisms even when provided for free (as in the case of automatically downloaded software patches). Researchers on a DARPA-funded project [13] developed “a mathematical model of the potential costs involved in patching and not patching at a given time”. They observed that the risk of loss of functionality from applying a bad patch decreases in time, while the risk of loss due to penetration while the patch is not applied increases with time. They hypothesized that the optimal time to apply the patch is when these curves cross, and developed a mathematical model (similar to the weighted ROI) that took into account various cost and probability factors. Using data collected from a study involving 136 patches, they were able to determine that at 10 and 30 days following a patch release, application is optimal. Of course, these intervals rely on some folks applying the (potentially bad or even bogus) patches sooner and reporting the defects they experienced – if everyone waits for the patches to be fixed, the time would be shifted forward, thus increasing early penetration risks.

There are also potential misuses of the CBA. Among these is in the application of the CBA to public-key cryptography in order to derive appropriate key sizes and expirations.

Silverman [14] asserts that a financial model, rather than a purely computational one, should be used to assess cryptographic vulnerabilities. He says “it makes no sense for an adversary to spend (say) \$10 million breaking a key if recovering the key will only net (say) \$10 thousand”.

The CBA has also not been without problems in terms of use and acceptance. One of the major impediments in the use of CBA is the complexity of the equations. This has been a problem in the business arena where CBA equations are considered more complex. Here, the models incorporate the use of risk-adjusted cash flows in order to examine internal rate of return (IRR) and maximum net present value (NPV) figured as a percentage of information security expenditures. Gordon and Loeb [15] explain that a simple return on investment (ROI) calculation that divides income by asset value is insufficient because it is based on historical rather than future valuations as affected by breach incidents. They use weighted annual expected loss estimates derived by multiplying the dollar value associated with potential breaches by the probability of occurrence for each breach. But they note that even the IRR and NPV metrics may be deficient because these compare the actual cost savings from the security investment to the anticipated cost savings, which “is difficult because the benefits of specific investments aren’t easily separated from other activities within a company. This is particularly relevant to security investments, the more successful the project, the less likely you are to see breaches”.

All of this presents the opportunity to broaden the scope and dept of cost-benefit analysis using a multi-faceted approach and also to address business process concerns in the hope that empiricism can shift the balance in favor of the consumers of computer security products and services. In the process, those “add-ons” and providers that do not demonstrably improve the security cost bottom line will be exposed and dispensed with. And as a necessity new tools and metrics that enable

risk and cost-benefit assessments will be developed and proliferated. Only through such independent quantification can we hope to get a true handle on the financial ramifications of security problems so that we might best direct our efforts toward resolving them.

With the above in mind, it needs to be pointed out that recent studies point to the direction of crafting new CBA techniques through interactive or adaptive techniques. Shawn [6] uses a cost-benefit analysis method called SAEM to compare alternative security designs in a financial and accounting information system. The goal is to help information-system stakeholders decide whether their security investment is consistent with the expected risks.

### **3. Implementation approaches**

Although there are many different approaches to intrusion detection, we believe that all of these variations can be categorized into two basic approaches, reactive and proactive. We will provide a context-based analysis on how each approach affects management cost in Section 6.3.

#### *3.1. Reactive approach*

We define a reactive approach as one in which response is done once personnel have been enlisted. Reactive approaches generally rely on techniques, such as cryptographic checksums or audit trail analysis mechanisms. A good example of a widely used UNIX IDS utility is Tripwire. Tripwire allows the files of a UNIX operating system to be cryptographically sealed for later review and comparison. If a file is modified, the checksum won't match, and an intrusion can be assumed. Several other passive IDS tools are available either as commercial products or as freeware/shareware. In almost every case, the tools provide a "post-mortem" of a security event or action. Since the tools don't monitor data transactions or other real-time events, they don't provide a means of preventing unauthorized intrusions. Instead, they provide a means to quickly respond to a security compromise, and in some cases, act as a deterrent to would-be system intruders.

#### *3.2. Proactive approach*

We define a proactive approach as one in which response is automated by the system. The proactive approach is based on active monitoring and analysis. Tools and utilities, using active techniques, monitor the actual data traffic, keystrokes, or other actions, and compare them against some predefined set of thresholds or rules. If a threshold or rule is exceeded, an alarm is activated. The key concept in active monitoring systems is that of real-time data collection, analysis, and alarms.

The distributed intrusion detection system (DIDS) is an example of proactive network-based IDS. DIDS is UNIX-based IDS that includes both agent software running on network hosts and a central security management console (the DIDS Director), where data is fused and alarms are generated in a graphical user interface. Developed by students at UC Davis, DIDS captures TCP/IP data traffic, in real time, and compares the collected traffic to stored “hacker profiles”. If the system detects a condition that appears to indicate an unauthorized intrusion, an alarm is generated at a console, much like a traditional network management system.

It should be noted that just because an IDS captures raw network traffic, it still might not provide active IDS capabilities. Many times, network-based IDS will capture packets or raw network traffic, store it to a file, and review it at a later date or time. In a recent analysis performed by Secure Networks, Inc. of several IDS products, most of the current product offerings were found to be based on passive IDS techniques.

Another approach to active intrusion detection is based on monitoring specific characteristics at the host operating system level, such as CPU utilization, memory utilization, input/output rates, etc. By creating a baseline (over time) of a system or collection of systems, these parameters can be monitored and measured to identify potential anomalous behavior. Since this data can be collected and analyzed in real time, it can be considered a proactive form of intrusion detection.

#### **4. Cost and management structures**

In order to prepare for the next section, we present a cost and management structure for IDS implementation in Section 4.1. Using a holistic approach, we analyze the cost aggregate for the different implementation schemes in Section 4.2.

##### *4.1. Implementation cost*

The associated cost of host-based intrusion detection systems (HIDS) deployments can vary depending on vendor and software versions. A good baseline is that agents can cost between \$500 and \$2000 each and consoles may cost in the \$3000–\$5000 range [16]. This does not always include OS, hardware or maintenance costs. Network intrusion detection systems can be deployed as stand-alone hosts with a possible management interface or distributed sensors and management console. Generally speaking, in the last couple of years commercially available sensors run in the \$5000–\$20000 area [16] depending on vendor, bandwidth and functional capabilities. Management consoles can be included free as part of the cost, or sold separately and can cost several thousand dollars depending on the vendor. This does not necessarily include hardware or back-end databases.

The total cost of implementing an IDS-based security solution depends on purchasing costs combined with the costs for managing the technology. Giving IDS

Table 2  
Cost of individual components [17]

Expense	Value (\$)
Network IDS	\$10 000
Host IDS	\$1000
Management station – NIDS and HIDS	\$5000 (may not apply for all products)
Maintenance	15% of the cost of NIDS and/or HIDS
MSSP network IDS management per year	\$24 000 (\$2K per month)
MSSP host IDS management per year	\$6000 (\$500 per agent per month)
Engineer cost	\$75 000 (\$60 000 salary plus \$15K benefits and admin)
Group manager cost	\$100 000 (\$80 000 salary plus \$20K benefits and admin)

Table 3  
Cost structures [17]

	Single support	24 × 7 × 365 Multi-shift support	MSSP support
Technology cost	\$24 650	\$24 650	\$24 650
Management cost	\$225 000	\$1 425 000	\$108 000
Total cost	\$249 650	\$1 449 650	\$132 650
Average cost per year	\$83 217	\$483 217	\$44 217
Average cost per device per year	\$27 739	\$161 072	\$14 739

management duties to a person not skilled in IDS technology is a poor idea. Some standard implementation and management methods common to IDS deployments include using a Managed Security Services Provider (MSSP), utilizing a single in-house employee or technician, or enabling 24 × 7 × 365 multi-shift coverage in-house with a skilled technical staff. Of course the size of the organization and its' associated IT budget (or lack thereof) factor in to how the IDS technology will be deployed and managed. Tables 2 and 3 represent the generalized cost structure that we will use for our discussion and case study.

#### 4.2. Comparative analysis of aggregate costs for different implementation schemes

An analysis of the aggregate costs for three different IDS deployments can be made based on the generalized cost structure in Tables 2 and 3. Tables 4 and 5 represent implementation (purchase) costs combined with life cycle management costs over a three-year period. The three scenarios include management by a single skilled in-house technician, management in which there are five shifts of skilled technicians providing 24 × 7 × 365 coverage, and management provided by an MSSP. It is very important to understand that full-service MSSPs will provide 24 × 7 × 365 coverage just like the multi-shift internal coverage provides. For completeness, we will review two different IDS deployments (one small and one medium) and consider the cost structure of implementing and managing them.

Table 4  
Implementation and management cost of one network IDS and two host IDS [17]

	Single support	24 × 7 × 365 Multi-shift support	MSSP support
Technology cost	\$24 650	\$24 650	\$24 650
Management cost	\$225 000	\$1 425 000	\$108 000
Total cost	\$249 650	\$1 449 650	\$132 650
Average cost per year	\$83 217	\$483 217	\$44 217
Average cost per device per year	\$27 739	\$161 072	\$14 739

Table 5  
Implementation and management cost of 15 network IDS and 15 host IDS [17]

	Single support	24 × 7 × 365 Multi-shift support	MSSP support
Technology cost	N/A	\$268 250	\$268 250
Management cost	N/A	\$1 425 000	\$1 350 000
Total cost	N/A	\$1 693 000	\$1 618 250
Average cost per year	N/A	\$564 417	\$539 417
Average cost per device per year	N/A	\$18 814	\$17 981

From the numbers it is evident that in smaller IDS deployments the value proposition of MSSP support is very strong relative to internal 24 × 7 × 365 multi-shift support. In larger IDS deployments, the cost differential between internal (highly skilled) multi-shift coverage and MSSP coverage diminishes due to economies of scale on the internal multi-shift coverage side. Single support coverage is not a realistic option to consider when contemplating a deployment of 30 security devices. Also, this cost model does not take into account proprietary tools development necessary to manage several different types of technology (if that were the case) effectively.

## 5. A case study on cost effective management approach

In this section we will use a hypothetical case study [16] to demonstrate the efficacy of the different management approaches. To do this we shall derive a value for the return on investment of each management method. The results will then be used to articulate a management framework.

### 5.1. Framework for risk analysis and ROI computation

Studies on suitable management approaches that maximize the IDS ROI are not clearly established. Therefore, the use of this case study approach will permit in-depth exploration of the benefits of illustrating ROI analysis in order to determine the management technique that maximizes the IDS deployment. From the case study, we hope to glean some general concepts about intrusion detection system ROI and

determine the most effective management approach that will maximize the return on investment. By developing the examples, we also hope to develop a possible method of reasoning about IDS cost effective management approaches more generally.

The case study will be presented in the context of the risk assessment and ROI studies given in Sections 5.4 and 5.5. In order to prepare for the studies, we set up a hypothetical company called ABC, Inc. and through the case study present the threat and incidence scenarios needed to calculate ROI – which is the indicator for effective implementation and lifecycle management of the IDS deployments.

Table 6  
ROI variables and risk equations

Variable	Formula or expression
Asset Value (AV)	$AV = \text{hardware} + \text{comm. software} + \text{proprietary software} + \text{data}$
Exposure Factor (EF)	EF is the % estimation of the exposure of the initial compromised asset
Underlying Exposed Assets (UEA)	UEA is the estimation of the \$ value of the assets behind the compromised initial asset
Secondary Exposure Factor (EFs)	EFs is the % estimation of the exposure of the UEAs
Cascading Threat Multiplier (CTM)	$CTM = 1 + ((UEA \times EFs)/AV)$
Single Loss Expectancy (SLE)	$SLE = EF \times AV \times CTM$
Annual Rate of Occurrence (ARO)	ARO is estimated number, based on available industry statistics or experience
Annual Loss Expectancy Without IDS (ALE1)	$ALE1 = SLE \times ARO$
Annual Loss Expectancy with IDS using auto-response (ALE2)	ALE2 = conservative 50% reduction of ARO when IDS is managed skillfully with auto-response
Annual Loss Expectancy with IDS using auto-response and incident response (ALE3)	ALE3 = conservative 25% reduction of EF and EFS when IDS is managed skillfully with auto-response and incident response
Annual Cost (T) of IDS Technology and Mgmt	T
Annual Recovery Cost (R) from Intrusions without IDS	$R = ALE1$
Annual Dollar Savings (E) gained by stopping intrusions with IDS	$E = ALE1 - (ALE2 \text{ or } ALE3)$
Traditional Return on Security Investment (ROSI) equation	$ROSI = R - ALE$ , where $ALE = (R - E) + T$
ABC, Inc. ROI of IDS with auto-response (ROI1)	$ROI1 = ALE1 - (((ALE1 - (ALE1 - ALE2)) + T)$
ABC, Inc. ROI of IDS with auto-response and incident response (ROI2)	$ROI2 = ALE1 - (((ALE1 - (ALE1 - ALE3)) + T)$

## 5.2. Risk assessment

A risk assessment (analysis) study [16] was conducted to quantify the loss associated with the occurrence of an incidence or a threat at ABC, Inc. In the analytical approach leading up to the calculation for ROI, commonly accepted formulas and definitions (Table 6) are used to calculate Asset Valuations (AV and UEA), Exposure Factors (EF and EFS), the single loss expectancy (SLE) and the Annual Rate of Occurrence (ARO). To fully explore the risk factors, three different scenarios of possible asset compromises were considered.

Procedurally, once the Asset Valuations (AV and UEA) and Exposure Factors (EF and EFS) have been calculated, the single loss expectancy (SLE) and the Annual Rate of Occurrence (ARO) are then computed. The Annual Rate of Occurrence (ARO) is computed based on the analysis of the annual frequency of threats and the computations for Asset Valuations (AV and UEA), and Exposure Factors (EF and EFS) and (ARO). The results of these calculations for our case study are shown in Table 7.

One of the results of the study is the recommendation to implement IDS technology to complement other security devices as a counter measure to future attacks. We now incorporate into our case study the different IDS implementation schemes described in Tables 4 and 5 in Section 4 in order to delineate the effect of each implementation scheme on the return on investment (ROI). The ROI will be the ultimate gauge of the effectiveness of the IDS management approach.

Consequently, in Section 5.3 we calculate the ROI using the data derived from the risk assessment study and IDS implementation management costs (for both single and MSSP support schemes) discussed in Section 4.

## 5.3. Return on investment

The formulas used for the ROI calculations are shown in Table 6. The support costs (\$83 217/year for single support coverage and \$44 217/year for MSSP support coverage) taken from the Table 4 are used in the ROI calculations. The results of the ROI calculation for the different IDS implementation are shown in Table 8.

## 5.4. Analysis of results

Auto-response affects primary mitigation windows, which has a direct impact on partially reducing the Annual Rate of Occurrence (ARO). This is illustrated [16] in the ROI Table 8 above, where a beneficial conservative reduction in ARO of 50% (highlighted in yellow in the "IDS w/Auto-Response" rows for each of the three scenarios) is attained. Incident response affects the secondary mitigation window, which impacts exposure factor (EF) and secondary exposure factor (EFS), which in turn impacts the Cascading Threat Multiplier (CTM). This is also illustrated in the ROI Table 8 above, where a beneficial conservative reduction in EF and EFS of

Table 7  
Calculations for asset valuations, exposure factors and annual rate of occurrence

Scenario	Descriptions of Compromised Asset (AV) and Underlying Exposed Assets (UEA)	Considerations in assigning estimates for Asset Valuations (AV and UEA), Exposure Factors (EF and EFS) and Annual Rate of Occurrence (ARO)	AV	EF	UEA	EFS	ARO
One	ABC, Inc. NT 4.0 Web server (AV); ABC, Inc. NT Domain (UEA)	Cost of lost productivity and revenue from downtime? Cost of compromised underlying data and assets? Cost of rebuilding web server? Potential cost of compromise of NT domain resources?	\$2000	75%	\$20 000	75%	3
Two	ABC, Inc. UNIX-based Web server (AV); old internal ABC, Inc. database containing inventory data and pricing for customers and suppliers (UEA)	Cost of lost productivity and revenue from downtime? Cost of loss of trust or confidence of ABC, Inc.'s online customers? Cost of compromised data and assets? Cost of rebuilding web server? Immediate cost of fulfilling current orders with whatever it takes to satisfy customers?	\$2000	50%	\$50 000	50%	2
Three	ABC, Inc. router; Primary supplier ABC, Inc.'s network	Cost of supply interruption from primary supplier? Cost of loss of trust or confidence of primary supplier? Potential cost of compromised data? Cost for ABC, Inc. to replace ACME as a supplier? Difference in credit terms for new supplier (compared to highly favorable terms that ABC, Inc. currently enjoys with ACME)? Difference in pricing between normal (new) supplier and ACME's pricing? Potential cost of litigation if ACME determines ABC, INC. employee is at fault? Cost of ABC, INC. compromise? Potential cost of liability for attacks directed at other non-partner networks?	\$3000	75%	\$200 000	50%	1

Table 8  
IDS ROI

Scenario	RQI scope	AV	EF	UEA	EFS	CTM	SLE	ARO	ALE1 (no IDS)	ALE2 (w/AR)	ALE3 (w/AR& IR)	Single support ROI		N5SP support ROI	
												\$	%	\$	%
One	no IDS	\$2000	75%	\$20 000	75%	8.5	\$12 750	3	\$38 250	N/A	N/A	N/A	N/A	N/A	N/A
	IDS	\$2000	75%	\$20 000	75%	8.5	\$12 750	1.5	\$38 250	\$19 125	N/A	-\$64 092	-77%	-\$25 092	-57%
	w/Auto-Response IDS	\$2000	56%	\$20 000	56%	6.6	\$7453	1.5	\$38 250	N/A	\$11 180	-\$56 147	-67%	-\$17 147	-39%
Two	w/Auto-Response and Incident Response														
	no IDS	\$20 000	50%	\$50 000	50%	2.3	\$22 500	2	\$45 000	N/A	N/A	N/A	N/A	N/A	N/A
	IDS	\$20 000	50%	\$50 000	50%	2.3	\$22 500	1	\$45 000	\$22 500	N/A	-\$60 717	-73%	-\$21 717	-49%
Three	w/Auto-Response and Incident Response														
	no IDS	\$3000	75%	\$200 000	50%	34.3	\$77 250	1	\$77 250	N/A	N/A	N/A	N/A	N/A	N/A
	IDS	\$3000	75%	\$200 000	50%	34.3	\$77 250	0.5	\$77 250	\$38 625	N/A	-\$44 592	-54%	-\$5592	-13%
	w/Auto-Response and Incident Response	\$3000	56%	\$200 000	38%	26.0	\$ 43 875	0.5	\$77 250	N/A	\$21 235	-\$27 905	-34%	\$11 096	25%
	WBS ROI with IDS Auto-Response (ROI1)								\$160 500	\$80 250	N/A	-\$2967	-4%	\$36 033	81%
	WBS ROI with IDS Auto-Response & Realtime Incident Response (ROI2)								\$160 500	N/A	\$47 648	\$29 635	36%	\$68 635	155%

25% respectively (highlighted in yellow in the “IDS w/Auto-Response and Incident Response” rows for each of the three scenarios) is attained.

These reductions have positive effects on the ROI of IDS. Once the aggregate annualized savings ( $ALE1 - ALE2$  or  $ALE1 - ALE3$ ) occurring from IDS deployment equals the support costs associated to the deployment, a positive ROI should materialize. In the case of ABC, Inc., the two ROIs (ROI1 and ROI2) for each support profile are as follows:

- Single support with IDS using auto-response (ROI1) = -4%;
- Single support with IDS using auto-response and incident response (ROI2) = 36%;
- MSSP support with IDS using auto-response (ROI1) = 81%; and
- MSSP support with IDS using auto-response and incident response (ROI2) = 155%.

These ROIs are based on the aggregate annualized savings from deploying and effectively managing the IDS technology and the resulting impact the IDS technology could reasonably have on the combined effect of the three compromise scenarios described above (see Table 7).

## 6. Propositions for cost effective management frameworks

The case study presented in the preceding section provides the insight needed to articulate the frameworks for a cost effective IDS management approach. From these, we propose the following management frameworks for the cost effective management of IDS deployments:

- Developing a composite metrics for cost estimates;
- Using local environmental factors to optimizing product selection;
- Implementation with the proactive and auto response mechanism; and
- Adopting a cost effective staffing and support structure.

### 6.1. Developing a composite metrics for cost estimates

Developing a composite metrics from known implementation cost items will in the longer run help establish a somewhat accurate budget for IDS management. Apart from the functional requirements, the IDS must also satisfy a number of economical requirements, in particular, cost. The following cost categories are integrated into the costs structure of IDS management [18]:

- Cost of the IDS product.
- Cost of additional computer resources needed.
- Cost of administration.

In addition, the costs components (technology, management, maintenance) described in Section 4.1 should be factored into the costs of acquiring additional computer resources and administration. Together all of this will be used to create an IDS cost metrics.

The importance of these cannot be under estimated. This will then become a reference for large, medium and small size enterprises, or indeed anyone trying to implement an IDS security solution.

## 6.2. Using local environmental factors to optimizing product selection

Iheagwara et al. [3] demonstrate that IDS performance is greatly influenced by IDS product selection for a given environment. The study investigates the relationship between different IDS products performance in varied network and traffic stream conditions; and also provides a side-by-side comparison of two different technologies for intrusion detection. One being older (Megabit IDS) and the other (Gigabit IDS) representing evolutions from pure megabit IDS to gigabit IDS based on the extension of recurrent characteristics of ID system to new technologies.

Given that Gigabit requirements will increasingly become mandatory especially for carrier networks that are associated with problems of data management and information overload, the results are significant because the data on which the techniques are evaluated represent a significant corpus of empirically obtained data. This can be used to simultaneously measure and evaluate the probability of detection of a given intrusion detection technique against that of another technique in order to compare the correct detection rates. Detection rates are among the many criteria used in selecting the most feasible IDS product.

Iheagwara et al. [3] demonstrate that the IDS performance in large-scale infrastructures is directly related to traffic and environmental characteristics.

Operationally, the requirements of an enterprise network that is deploying a few devices locally to watch over a class-C network is going to be different from that of a multi-national corporation that is deploying hundreds of devices. The requirements should tie known performance values with the IDS product selection. In this regard, a clear delineation of the traffic load in order to estimate the type or number of a particular IDS product that will match expected performance level should precede the management approach.

In a different study, Iheagwara et al. [2] provide justification that an effective ID system can be achieved by using a best effort delivery/deployment approach that integrates the monitoring and deployment techniques to maximize the benefits of the ID system. The effectiveness of the IDS is closely linked to various factors including network topology, deployment techniques, and network throughput, bandwidth and network traffic conditions.

The conclusions drawn from the studies are that IDS product selection should be based on local factors. Comparatively, cost and other techno-economic factors should determine the product type and the implementation technology.

### 6.3. Implementation with the proactive and auto response mechanism

The concepts of proactive and reactive management techniques have been explained in Section 2 above. The sequence of events for each technique is explained in Table 9.

By examining the Annual Loss Expectancy ( $ALE = ARO * SLE$ , where  $SLE = Exposure\ Factor * Asset\ Value * Cascading\ Threat\ Multiplier$ ) we can determine which variables are affected by each of these two management methods. In a reactive design, where personnel must be engaged to respond to each event, the exposure factors (primary [EF] and secondary [EFs]) will be affected. In a proactive design there will be similar benefits to the exposure factors (re: a reduction) and, in addition, the Annual Rate of Occurrence (ARO) will be influenced in a beneficial way as well. To demonstrate the impact of threat vs. time we will use the concept of primary and secondary mitigation windows. In Fig. 1, the primary mitigation window affects ARO while the secondary mitigation window affects Exposure Factor and Cascading Threat Multiplier [16]. CTM factors in the importance of other critical assets tied (re: networked) to the specific asset being analyzed in the ALE calculation. An effective way of impacting ARO is through automated response.

Auto-response can take many forms. On host-based IDS this is sometimes called shielding, where a specific process is terminated. Network-based IDS generally employs TCP resets or shunning. TCP resets effectively kills one specific session based on suspicious activity, but it still allows other activity from that same IP. Shunning, on the other hand, changes firewall rules or router access lists and effectively denies all traffic from that host for a specific period of time. In essence, shielding will protect a single host from one process, resets will protect a host from a specific session, and shunning will protect the entire network from a specific host for a pre-determined amount of time.

The accuracy of automated response can vary tremendously. This is dependent on the skill level of the engineers managing the devices. If the engineers are moderately skilled then auto-response will not be very effective, which may adversely affect the ROI of the IDS deployment. This adverse effect may manifest itself in the form of a loss of productivity from network-related problems due to improperly implemented auto-response, as well as the additional fallout related to a false sense of security throughout the company. It is assumed that a moderately skilled engineer is one who has gone through a formal process of training on intrusion detection systems operation and must have managed or operated the device for at least twelve (12)

Table 9  
Proactive and reactive management methods

Method	System actions	Personnel actions	Follow up information
Reactive	Log → Alert →	Respond → Analyze → Eradicate	Forensics and Evidence
Proactive	Respond → Log → Alert	Analyze → Eradicate if necessary	Forensics and Evidence

months while a highly skilled engineer is one who in addition to the above have managed and operated the device for at least twenty-four (24) months.

With skilled engineers managing the devices, we believe auto-response can be very accurate and effective. Because few statistics exist that illustrate the accuracy of automated response the statistics [16] generated from our analysis of one month's worth of data on NetSolve, Incorporated networks will be used for the illustration. If we include Code Red and Nimda activity, in 99.96% of the attacks, where automated response was used to mitigate the threat, the activity was malicious. Excluding large-scale worms, the attacks were malicious in 95.8% of auto-response uses. Of the 4.2% of the traffic that was not malicious, not all of it was desirable. Some of this traffic was peer-to-peer programs, on-line gaming, chat and other undesirable traffic that triggered alarms. The percentage of traffic that was denied that was business related was very small. It should be noted that many of these devices provide numerous different techniques for ensuring that very little, if any, legitimate traffic is denied through the use of automated response.

To determine how effective the device is in recognizing attacks we will use the most recent results [19]. In this test the worst NIDS detected 67 of 109 attacks or 61.5%, while the best detected 94 of 109 attacks for an 86.2% detection rate. Even the worst case, the 61.5% detection rate was out of the box [20] and it was reported that it would not be difficult to improve this with some custom signatures and tuning. What does all this mean? It means that the worst IDS tested can still detect at least

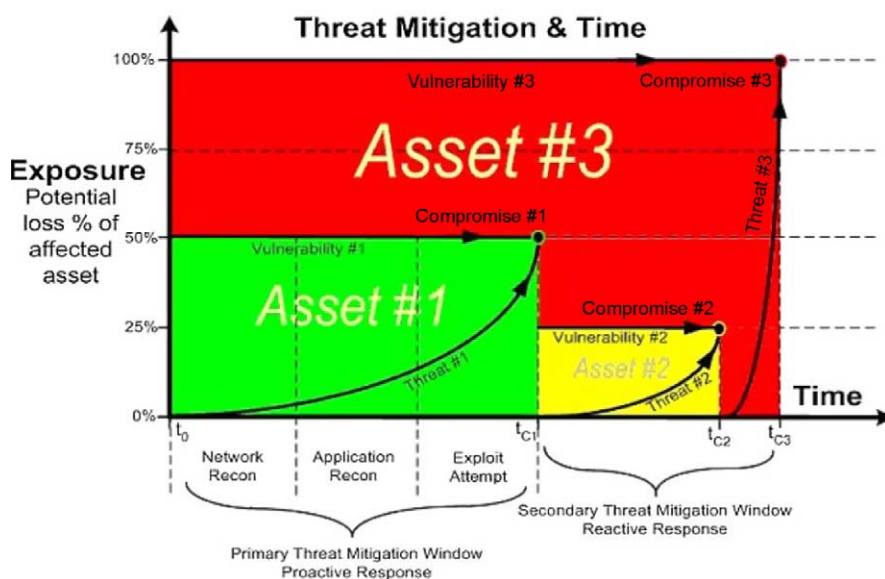


Fig. 1. Threat mitigation window [16].

61.5% of attacks. Realistically that number should be closer to 70% when a skilled engineer or technician manages the device.

The cost benefit is that the auto-response feature, when properly used, can be a very effective method of reducing the Annual Rate of Occurrence (ARO).

#### 6.4. Adopting a cost effective staffing and support structure

The results of the studies in Section 5 demonstrate that the use of auto-response scheme produces by far better return on investment in both NIDS and HIDS deployments. A conservative estimate of 50% reduction in ARO is facilitated by the utilization of auto-response. Also, the 25% reduction in both exposure factors (EF and EFS) should also be considered a conservative estimate in the IDS deployment with auto-response and prompt incident response scheme.

The benefits of a better IDS management are reflected in the reductions in the values of the variables (see highlighted cells under ARO, EF and EFS in Table 8). The overall effect is visible in the increase in the ROI values for the ABC, Inc. IDS deployment for both the single in-house support and MSSP support schemes.

In the final analysis, attainment of a better ROI depends on a good management practice especially the use of highly skilled engineers or technicians that have a sound understanding of the technology including the inherent strengths and weaknesses to manage the IDS technology. It is also a reasonable assumption that a single in-house engineer or technician would better support IDS deployment of one NIDS and two HIDSs. On the other hand, it will be ineffective to assume that one person can support this highly dynamic technology on a continual 24/7/365 basis with active auto-response and real-time incident response for every security event. Multi-shift internal support as well as Managed Security Service Provider (MSSP) support is the preferred ways of providing definitive 24/7/365 support and real-time incident response.

## 7. Conclusions

The decision to deploy a security mechanism such as IDS is often motivated by the needs of security risk management. As a matter of reality, a very important but often neglected facet of intrusion detection is its *cost-effectiveness*, or *cost-benefit* trade-off. The objective of IDS is therefore to provide protection to the information assets that are at risk and have value to an organization. For IDS to be cost-effective, it should cost no more than the expected level of loss from intrusions. This requires that the IDS consider the trade-off among cost factors, which at the minimum should include development cost, the cost of damage caused by an intrusion, the cost of manual or automatic response to an intrusion, and the operational cost, which measures constraints on time and computing resources. For example, an intrusion that has

a higher response cost than damage cost should usually not be acted upon beyond simple logging.

The effectiveness of intrusion detection systems (IDS) is dependent upon an organization's deployment strategy and how well the successful implementation and management of the technology helps the organization achieve the tactical and strategic objectives it has established. One such strategic objective could be a positive Return on Investment (ROI). For organizations interested in quantifying the IDS's value prior to deploying it, their investment decision will hinge on their ability to demonstrate a positive ROI. ROI has traditionally been difficult to quantify for network security devices, in part because it is difficult to calculate risk accurately due to the subjectivity involved with its quantification. Also, business-relevant statistics regarding security incidents are not always available for consideration in analyzing risk.

In considering an implementation of IDS technology, a return on investment can be understood by analyzing the difference between annual loss expectancy (ALE) without IDS deployment and the ALE with IDS deployment, adjusted for technology and management costs. The ultimate initial goal, then, should be to prove that the value proposition (re: a benefit in the form of a quantifiable reduction in ALE) in implementing and effectively managing the IDS technology is greater than the implementation and management costs associated with deploying the IDS technology.

Finally, this paper has demonstrated that effective management methods will maximize the performance of the IDS and that a positive IDS ROI is attainable with an effective deployment technique and optimal management approach.

## Acknowledgements

The contributions of Kevin Timm and David Kinn of Security Engineers at Netsolve, Inc., Austin, USA are gratefully acknowledged.

We also gratefully acknowledge Dr. Deborah Frincke's constructive suggestions on the improvement of this paper.

## References

- [1] K. Richards, Network based intrusion detection: a review of technologies, *Computers & Security* **18** (1999), 671–682.
- [2] C. Iheagwara et al., Evaluation of the performance of IDS systems in a switched and distributed environment, *Computer Networks* **39** (2002), 93–112.
- [3] C. Iheagwara et al., A comparative experimental evaluation study of intrusion detection system performance in a gigabit environment, *Journal of Computer Security* **11**(1) (2003).
- [4] W. Lee et al., *Toward Cost-Sensitive Modeling for Intrusion Detection and Response*, North Carolina State University, 1999.

- [5] S. Stolfo et al., Cost-Based Modeling for Fraud and Intrusion Detection Results from the JAM Project, Technical Report, Columbia University.
- [6] S.A. Butler, Security attribute evaluation method: A cost-benefit approach, in: *Proceedings of the International Conference on Software Engineering*, Orlando, FL, 2002.
- [7] H. Wei et al., Cost benefit analysis for network intrusion detection systems, in: *Proceedings of the CSI 28th Annual Computer Security Conference*, Washington, DC, October 2001.
- [8] C. Irvine et al., Toward a taxonomy and costing method for security metrics, in: *Proceedings of the Annual Computer Security Applications Conference*, Phoenix, AZ, 1999.
- [9] Cohen et al., A preliminary classification scheme for information system threats, attacks, and defenses; a cause and effect model; and some analysis based on that model, *Sandia National Laboratories*, September, 1998.
- [10] Federal Information Processing Standards, *Guideline for the Analysis of Local Area Network Security*. National Institute of Standards and Technology, FIPS PUB 191, November 1994; <http://www.itl.nist.gov/fipspubs/fip191.htm>.
- [11] R. Clarke, Computer matching by government agencies: The failure of cost/benefit analysis as a control mechanism, *Information Infrastructure and Policy* 4, 1 (March) (1995); <http://www.anu.edu.au/people/Roger.Clarke/DV/MatchCBA.html>.
- [12] NIH's Cost-Benefit Analysis Guide for NIH IT Projects. Available at: <http://www.oir.nih.gov/itmra/cbaguide.doc>.
- [13] A. Beattie et al., Timing the application of security patches for optimal uptime, in: *Proceedings of LISA'02: Sixteenth Systems Administration Conference*, USENIX Association, 2002.
- [14] R.D. Silverman, A cost-based security analysis of symmetric and asymmetric key lengths, *RSA Laboratories Bulletin* 13 (April) (2000).
- [15] L. Gordon et al., Return on information security investments: Myths vs. realities, *Strategic Finance Magazine* (Nov.) (2002); <http://www.strategicfinancemag.com/2002/11i.htm>.
- [16] T. Kevin et al., CTM, Technical Report, Netsolve, Inc., Austin, USA, 2002.
- [17] C. Iheagwara, The effect of intrusion detection management methods on the return on investment, *Computers & Security Journal* (October) (2003) (accepted).
- [18] H. Debar et al., Towards a taxonomy of intrusion-detection systems, *Computer Networks* 31 (1999).
- [19] [http://www.silicondefense.com/software/acbm/speed\\_of\\_snort\\_03\\_16\\_2001.pdf](http://www.silicondefense.com/software/acbm/speed_of_snort_03_16_2001.pdf).
- [20] <http://www.nss.co.uk/Articles/IntrusionDetection.htm>.

Copyright of Journal of Computer Security is the property of IOS Press and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.