

Justifying the Expense of IDS, Part One: An Overview of ROIs for IDS

Kevin Timm 2002-07-18

Justifying the Expense of IDS, Part One: An Overview of ROIs for IDS

by David Kinn and Kevin Timm

last updated July 18, 2002

Introduction

A positive return on investment (ROI) 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. 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 to deploying the IDS technology. We will examine how implementation methods, management methods, and IDS policy affect ROI. This article will seek to demonstrate the value associated with a well thought out implementation and effective lifecycle management of IDS technology and will culminate (in Part II) with a number crunching exercise to calculate the ROI for an IDS deployment by a hypothetical brick n' mortar wholesale hardware supply company named Wally's Building Supplies (WBS), Inc.

HIDS and NIDS Advantages

Intrusion Detection is really an overlay of two separate and different technologies. Intrusion detection systems are divided into two types: Network IDS (NIDS) and Host-based IDS (HIDS) systems. The primary advantage of NIDS is that it can watch the whole network or any subsets

of the network from one location. Therefore, NIDS can detect probes, scans, malicious and anomalous activity across the whole network. These systems can also serve to identify general traffic patterns for a network as well as aid in troubleshooting network problems. When enlisting auto-response mechanisms, NIDS can protect independent hosts or the whole network from intruders. NIDS does, however, have several inherent weaknesses. These weaknesses are its susceptibility to generate false alarms, as well as its inability to detect certain attacks called false negatives. NIDS also is not able to understand host specific processes or protect from unauthorized physical access. HIDS technology overcomes many of these problems. However, HIDS technology does not have the benefits of watching the whole network to identify patterns like NIDS does. A recommended combination of host and network intrusion detection systems, in which a NIDS is placed at the network border and an HIDS is deployed on critical servers such as databases, Web services and essential file servers, is the best way to significantly reduce risk.

Generally speaking, most of these host-based systems have common architectures, meaning that most host systems work as host agents reporting to a central console. The associated cost of 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. This does not 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, commercially available sensors run in the \$5000-\$20,000 area depending on vendor, bandwidth and functional capabilities. Management consoles can be free or can cost several thousand dollars depending on the vendor. This does not necessarily include hardware or back-end databases.

How much is that IDS Management in the window?

The total cost of an IDS deployment depends on implementation costs combined with the costs for managing the technology. Giving IDS management duties to a person not skilled in IDS technology is a poor idea that will be covered later in the article. 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 24x7x365 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. The following table represents the generalized cost structure that we will use for our discussion.

Cost Structure

Expense	Value (\$)
Network IDS	\$10,000
Host IDS	\$1,000
Management Station - NIDS & HIDS	\$5,000 (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	\$6,000 (\$500 per agent per month)
Engineer Cost	\$75,000 (\$60,000 salary plus \$15K benefits & admin)
Group Manager Cost	\$100,000 (\$80,000 salary plus \$20K benefits & admin)

Based on this generalized cost structure, let's now consider the aggregate costs of three different IDS deployments. The chart below represents 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 24x7x365 coverage, and management provided by an MSSP. It is very important to understand that full-service MSSPs will provide 24x7x365 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.

Implementation & Management of one Network IDS and two Host IDS

	Single Support	24x7x365 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

Implementation & Management of 15 Network IDS and 15 Host IDS

	Single Support	24x7x365 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 24x7x365 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.

Mechanics of Risk

In order to prepare for the next section, where we will set up our hypothetical company and calculate ROI based on the effective implementation and lifecycle management of HIDS and NIDS technologies, we will need to articulate the holistic approach we are considering for analyzing risk and, at the same time, introduce some new concepts along the way. In our analytical approach working up to the calculation for ROI, we will use commonly accepted formulas and definitions associated with asset valuation, exposure, threat, vulnerability and loss expectancy. The Cascading Threat Multiplier (CTM), an additional factor we've added to the mix, enables us to expand on the widely accepted calculation for Single Loss Expectancy (SLE) where, traditionally, $SLE = Exposure\ Factor\ (EF) \times Asset\ Value\ (AV)$.

In order to stress the importance of the intangible considerations that will help us apply our holistic approach for quantifying risk and calculating a meaningful ROI, the concepts of goodwill and opportunity costs should be considered when performing valuation exercises on company assets. Although intangible factors inherently introduce subjectivity into risk and return analysis, it is nonetheless an important step to consider intangibles before one can arrive at a more meaningful calculation of ROI. It is worth mentioning here that, in general, it may be safe to

assume that organizations would tend to undervalue certain data assets if they have not fully taken into account (or bothered to understand for that matter) how these assets relate to the "big picture". It is simple human nature to take the path of least resistance when given a choice. But that's a very dangerous path to take for anyone attempting to arrive at an accurate assessment of the value of data assets residing on their network. Understanding the tangible costs and benefits of an asset is much easier than understanding, or even considering for that matter, the intangible costs and benefits associated to that same asset. Clarifying this understanding is one of our challenges and one we will address throughout the rest of the article as we work toward calculating the IDS ROI for Wally's Building Supplies, Inc.

The following commonly accepted formulas and definitions for our risk and return analysis were obtained from various sources on the Web and in print. All definitions in italics are direct quotes taken directly from these sources.

- Asset Value (AV) = hardware + comm. software + proprietary software + data

"One can measure an informational assets value by estimating the development, purchasing, licensing, supporting and replacement costs associated with the resource. Value can also be measured [from an] organizational [as well as] an external market [perspective]." (From the [StrongBox Security™ Web site](#))

- Exposure Factor (EF)

"The Exposure Factor represents the percentage of loss that a realized threat could have on a specific asset [when the specific threat matches up with a specific vulnerability]."(From the [StrongBox Security™ Web site](#))

"A threat is a single event that has the potential to cause damage to an asset. The threat usually [manifests itself] through [a] vulnerability in the information system."(From the [StrongBox Security™ Web site](#))

A vulnerability is a known or unknown weakness that can be exploited by any number of known or unknown threats.

- Single Loss Expectancy (SLE) = EF x AV

"In the end, risk is evaluated in terms of money. This is true even if life is lost; in the case of loss

of life, it may be a lot of money. For any threat we have defined, we take the value of assets at risk and multiply that by how exposed they are. This yields the expected loss if we were to get clobbered by the threat. This is called the single loss expectancy (SLE)." From Network Intrusion Detection; An Analyst's Handbook, 2nd Edition by Stephen Northcutt and Judy Novak

- Annual Loss Expectancy (ALE) = SLE x ARO

"The Annual Loss Expectancy is the annually expected financial loss to an asset resulting from one [specific] threat."(From the [StrongBox Security™ Web site](#))

"The Annual Rate of Occurrence (ARO) is the estimated number of times a threat on a single asset is estimated to occur. The higher the risk [associated to the threat] the higher the Annual Rate of Occurrence."(From the [StrongBox Security™ > Web site](#))

Now let's introduce a new concept, Cascading Threat Multiplier (CTM), into the mix. This will greatly aid us in our analytical discussion and move us further along in distilling a meaningful ROI calculation that can help us determine the effectiveness or ineffectiveness of deploying IDS technology into a given network.

The Cascading Threat Multiplier (CTM) is a multiplying factor that will be included into our expanded definition of Single Loss Expectancy (SLE). CTM is somewhat subjective and is introduced mainly for the purpose of adding a little more "flavor" to SLE. CTM factors in the importance of other critical assets tied (re: networked) to the specific asset being analyzed in the SLE calculation. It also coaxes us to think in broader terms and look at the bigger picture when considering the risks associated to the compromise of a given asset. The formula for CTM is as follows:

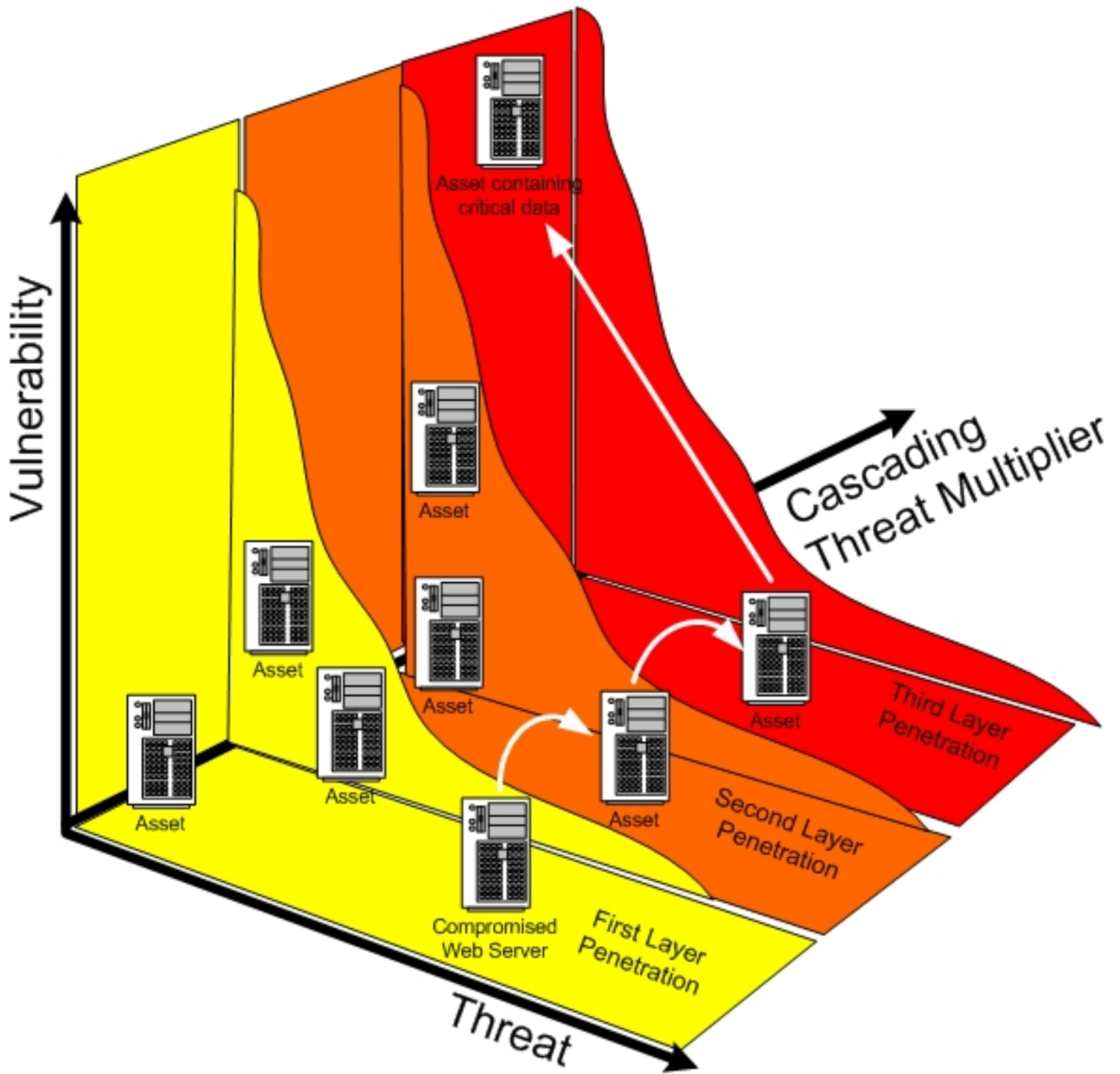
- Cascading Threat Multiplier (CTM) = 1 + ((UEA x EFS) / AV)

In this formula, Underlying Exposed Assets (UEA) is measured in dollars. These are the assets that are now exposed due to the compromise of a specific asset. Asset Value (AV) is identical to the calculation previously described above. Exposure Factor (EFS) represents secondary exposure factor and is related to the percentage loss on the UEAs. Secondary Exposure Factor (EFS) is very similar to Exposure Factor (EF), as previously described in the standard equation above, with a few minute differences. The primary reason for introducing EFS is to factor in the importance of an assets logical location within a network. For example, if the asset is a Web server that is in a true DMZ and has no access into the network or to any other corporate

servers, EFS would be low since it is unlikely that an attacker can use this device to further compromise the network. But if the asset is on the same broadcast domain as other servers are on (such as e-mail, DNS and FTP), or there is no access control between the asset and other servers, then EFS will be higher. Finally, if the asset is on a network that has access to the rest of the network, then Secondary Exposure Factor (EFS) will be very high. Examples of this would include hosts that offer some public services but are terminated within the internal network or hosts that have valid SSH keys to all other hosts.

It is important to consider what assets are easily (or even not so easily) accessible from a specific networked asset once that asset is compromised. When a given asset is compromised and used as a staging point for attacks on other assets inside and outside a company's network, it could have potentially devastating consequences for the organization. If an attack is staged from the compromised asset to another asset outside the organization, even when the owner was not directly involved in the malicious activity, they can and probably will be held accountable. One can envision the UEA factor of SLE representing some portion of a trusted business partner's assets. It is easy to imagine the negative business impact the offending organization would encounter if one of their compromised assets were used as a staging ground to compromise and damage their business partner's assets. What is the risk, quantified in dollars, of not considering a business partner's assets when performing a valuation exercise on your company's assets, ones that, if compromised, may enable access to more sensitive data and systems? The CTM concept reminds us to closely scrutinize the assets under our control, assign more comprehensive valuations to those assets, and more accurately try to measure the impact that their compromise could have on the organization.

Let's assume that a Web server is compromised and used by a malicious person to stage attacks on other networked assets containing critical data valued at 10 times the amount (in dollars) of the data contained on the compromised Web server. As the perpetrator hop-scotches his way from asset to asset, penetrating deeper and deeper into the network, he may finally gain access to critical data on a vulnerable asset deep inside the company's network. The CTM for the Web server would be calculated as follows if we surmise (re: best guess or WAG) that the secondary exposure factor (EFS) of the Underlying Exposed Asset(s) (UEA) is 70%: $CTM = 1 + ((10 * .7) / 1) = 8$. The CTM has increased the SLE for the compromised Web server by a factor of 8. Follow the white arrow originating from the compromised Web server to better visualize this concept.



Tying the CTM concept back into our SLE calculation, our new definition of Single Loss Expectancy is as follows:

- $SLE = EF \times AV \times CTM$

Thorough security professionals may have already factored in our CTM concept by executing a more comprehensive valuation methodology that included more subjective, intangible factors into their Asset Value (AV) variable calculation. As mentioned above, goodwill (i.e. business and

consumer loyalty built on trust) and opportunity costs (i.e. choosing not to consider the effect that a compromised asset can have on other assets) are somewhat analogous to our CTM concept when these intangibles are factored into the Asset Valuation (AV) used in the SLE calculation. The importance of capturing intangible value, and understanding the risks associated to jeopardizing that value, is one of the more challenging aspects of risk and return analysis. By introducing our CTM concept into the traditional SLE calculation we are attempting to make the capture of the intangible aspects of asset valuation a little less daunting of a task.

Finally, let's come full circle now and tie the risk analysis calculations listed above to an accepted formula for calculating ROI for security

- Return on Investment (ROI) = Recovery Cost (R) - ALE, where $ALE = (R - E) + T$, where E equals the \$ savings gained by stopping an attack and T equals the cost of a security product. ("Security still a 'Net lifestyle issue" by site M.H. (Mac) McMillan, April 8th, 2002, Reprinted from tech.first, a special publication of Business First.)

Conclusion

In Part Two of this series, we will outline our sample company Wally's Building Supplies, Inc. and plug in all the numbers to calculate the return on investment for various implementations and lifecycle management techniques based on the three scenarios and cost structures described above. Stay tuned...

Kevin Timm is a Security Engineer at NetSolve, Inc.

David Kinn is a Project Manager for ProWatch Secure services at NetSolve, Inc.

[Privacy Statement](#)

Copyright 2006, SecurityFocus