Forrester Consulting

MAKING LEADERS SUCCESSFUL EVERY DAY

FORRESTER®

Prepared for SecureWorks

March 2008

The Total Economic Impact™ Of SecureWorks' Security Information And Event Management Service

Project Director: Michelle Salazar, Consultant

Contributors: Jeffrey North, Senior Consultant

FORRESTER

Headquarters

Forrester Research, Inc., 400 Technology Square, Cambridge, MA 02139 USA

Tel: +1 617.613.6000 • Fax: +1 617.613.5000 • www.forrester.com

TABLE OF CONTENTS

Executive Summary

In December 2007, SecureWorks commissioned Forrester Consulting to examine the total economic impact and potential return on investment (ROI) that enterprises might realize from deploying SecureWorks' Security Information and Event Management (SIEM) Service.

SecureWorks provides services that enable organizations to protect their critical information assets from digitally borne threats and vulnerabilities. The company provides managed security and consulting services that help security professionals across an extensive base of enterprise clients develop effective threat and vulnerability management programs. SecureWorks' services — which deliver enhanced security, improved compliance, and greater operations efficiency as well as reduce security program costs — include:

- Security device management.
- Enterprise security monitoring.
- Security information and event management.
- Vulnerability scanning.
- Threat intelligence.
- Consulting services.

Pacific Gas and Electric Company (PG&E), one of the largest natural gas and electric utilities in the United States, uses SecureWorks' SIEM Service at the monitoring level for more than 90 systems in its network. In in-depth interviews with PG&E, Forrester found that the organization achieved comprehensive, enterprise-level security monitoring at a lower cost than the alternative of implementing and maintaining an in-house 24x7 Security Operating Center (SOC) and SIEM solution. PG&E also achieved a lower risk of loss due to security breaches, and was better able to track security performance for audits and reporting, thus building credibility for their security program within the organization and with clients.

Forrester calculated that PG&E achieved a return on investment (ROI) of 193%, with a nearly immediate payback period.

Purpose

The purpose of this study is to provide readers with a framework for evaluating the potential financial impact of SecureWorks' SIEM Service on client organizations. Forrester's aim is to clearly show all calculations and assumptions used in the analysis. Readers should use this study to better understand and communicate a business case for investing in SecureWorks/SecureWorks' SIEM Service.

Methodology

SecureWorks selected Forrester for this project because of its industry expertise in enterprise security technologies and threat management and Total Economic Impact™ (TEI) methodology. Forrester's TEI not only measures costs and cost reduction (areas typically accounted for within IT),

but also weighs the enabling value of a technology with respect to increasing the overall effectiveness of business processes.

Forrester employed four fundamental elements of TEI in modeling SecureWorks' SIEM Service:

1. Costs.
2. Benefits to the entire organization.
3. Flexibility.
4. Risk.

Given enterprises' increasing sophistication regarding cost analyses related to IT investments, Forrester's TEI methodology serves a useful purpose by providing a complete picture of the total economic impact of purchase decisions. See Appendix A for additional information on the TEI methodology.

Approach

Forrester used a four-step approach for this study:

1. Gather data from existing Forrester research relevant to security and threat management.
2. Interview SecureWorks' marketing and product development personnel in order to fully understand the value proposition of SecureWorks' SIEM Service.
3. Conduct a series of in-depth interviews with an enterprise client that has engaged SecureWorks' SIEM Service.
4. Construct a financial model representative of the interviews described in the TEI Framework section below.

Key Findings

Forrester's study yielded the following key findings:

- **ROI.** Based on interviews with Pacific Gas and Electric Company (PG&E), Forrester constructed a TEI framework for the organization and the associated ROI analysis to illustrate the areas of financial impact. As seen in Table 1, the ROI for our composite company is 193% with an almost immediate breakeven point (payback period).
- **Benefits.** The main quantified benefits for PG&E were: 1) the lower cost associated with outsourcing security monitoring to SecureWorks compared with establishing and maintaining an in-house SOC and SIEM solution; 2) cost avoidance in development fees; and 3) lower risk of loss due to security breaches because of a more robust, enterprise-level view of security monitoring. Forrester conservatively estimates the value of these benefits at $8,537,115 (present value) over three years.
- **Costs.** The costs of implementing SecureWorks SIEM Service include: 1) the monthly fee for the service; 2) account maintenance and administration; and 3) internal pre-planning effort. Forrester estimates the total of these costs at $2,910,069 (present value) over three

years, monthly service being the main component. The SecureWorks' SIEM Service fee for an organization like PG&E at the selected service level is $1,140,000 per year.

Table 1 illustrates the risk-adjusted cash flow for the composite organization based on data and characteristics obtained during the interview process. Forrester risk-adjusts these values to take into account the potential uncertainty that exists in estimating the costs and benefits of a technology investment. The risk-adjusted value is meant to provide a conservative estimate that incorporates any potential risk factors that might later affect the original cost and benefit estimates. In-depth explanations of risk and risk adjustments as used in this study can be found in the Risk section.

Table 1: PG&E ROI, Risk-Adjusted

Summary of Financial Results	Original Estimate	Risk-Adjusted
ROI	206%	193%
Total costs (PV)	($2,910,069)	($2,910,069)
Total benefits (PV)	$8,901,578	$8,537,115
Total (NPV)	$5,991,508	$5,627,046

Source: Forrester Research, Inc.

Disclosures

The reader should be aware of the following:

- The study is commissioned by SecureWorks and delivered by the Forrester Consulting group.
- SecureWorks reviewed the results and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.
- The customer for the interviews was provided by SecureWorks.
- Forrester makes no assumptions about the potential return on investment other organizations might realize. Forrester strongly advises that readers use their own estimates within the framework provided in the report to determine the appropriateness of an investment in SecureWorks/SecureWorks' SIEM Service.
- This study is not meant to be used as a competitive product analysis.

SecureWorks' SIEM Service: Overview

Service

According to SecureWorks, the company delivers a breadth of security services 24x7x365 through its proprietary Sherlock Platform augmented with applied security research and GIAC-certified experts. SecureWorks' SIEM Service enables clients to realize the benefits of a SIEM service without the drawbacks of having to implement, maintain, and effectively manage highly complex SIEM software products. SecureWorks' SIEM Service delivers event aggregation, correlation, and reporting "in-the-cloud," and immediately presents clients with actionable information, a

consolidated view of the security status of their critical assets, and on-demand reports to demonstrate compliance.

SecureWorks' SIEM Service is ideal for assets that require reports for audit or compliance purposes. SecureWorks provides log monitoring and analysis and delivers SIEM "in-the-cloud" without the need to deploy on-site SIEM software and infrastructure. The services are integrated throughout the Sherlock Platform, enabling customers to generate comprehensive reports across all services using Sherlock's client interface. This also enables customers to leverage the expertise of SecureWorks' GIAC certified staff for any security issue whether the assets in question are under the customer's monitoring service or SecureWorks' SIEM Service. Additionally, the customer is able to escalate incidents from the SecureWorks' SIEM Service back to SecureWorks' SOC staff for further analysis and mitigation assistance at any time without incurring additional fees.

There are three service levels currently available to customers of SecureWorks' SIEM Service: Managed, Monitored, and Self-Service.

Infrastructure

SecureWorks' Secure Operation Centers. SecureWorks Inc.'s secure operation centers (SOCs) — located in Atlanta, GA, Myrtle Beach, SC, and Chicago, IL — are fully redundant and provide seamless failover in case of emergency. SecureWorks' SOCs are staffed by SecureWorks' team of intrusion analysts who hold SANS Institute Global Information Assurance Certifications (GIAC) and have an average of three and one-half years experience as intrusion analysts. Also residing at the SOCs are members of SecureWorks' Counter Threat Unit, an industry-recognized team of security researchers. The team identifies and analyzes emerging threats to evaluate the risks they pose to client environments and develops countermeasures to protect clients' critical information assets.

Sherlock Security Management Platform. The Sherlock Security Management Platform is SecureWorks' proprietary SIEM technology developed specifically for the purpose of providing best-of-breed managed security services to thousands of enterprises simultaneously. The platform provides all the benefits of SIEM including robust asset-based reporting, workflow tools, and holistic security information without requiring investment in on-site infrastructure like specialized databases and servers. Additionally, SecureWorks can remotely eradicate malware identified in a client environment using its Web-based Paramedic technology.

Analysis

As stated in the Executive Summary, Forrester used a multistep approach to evaluate the impact of implementing SecureWorks' SIEM Service on an organization:

- Interviews with SecureWorks marketing and technical personnel.
- Review and analysis by a Forrester analyst whose focus includes enterprise security and other relevant technology.
- In-depth interviews with an enterprise client that has implemented SecureWorks' SIEM Service.
- Construction of a financial framework around the implementation of SecureWorks' SIEM Service.

Interview Highlights

Pacific Gas and Electric Company (PG&E) is one of the largest combination natural gas and electric utilities in the United States. A subsidiary of PG&E Corporation, it serves approximately 15 million people in northern and central California and has more than 20,000 employees and annual revenues in excess of $15 billion.

In a recent 2007 INFOSEC Assessment administered by the National Security Agency (NSA), PG&E received an overall IA-CMM Ratings Profile of Level 3, the second highest rating ever given out by the NSA in the INFOSEC Assurance-Capability Maturity Model (IA-CMM) category. PG&E is also the only utility worldwide to acquire an IA-CMM rating. PG&E was assessed by the NSA on measures of quality and maturity in nine process areas related to performing INFOSEC assurance services.

PG&E first engaged SecureWorks' SIEM Service in 2005 at the SecureWorks Monitored level of service, which guarantees 24x7 security event and log monitoring, and analysis and response for detection server event logs, firewalls, routers, and other non-managed devices. The Monitored SLA level includes device monitoring, unlimited access to SecureWorks' analysts, no limits on device changes, and no additional charges beyond the monthly service fee.

The in-depth interviews with PG&E revealed that:

- PG&E uses SecureWorks for more than 1,000 devices including servers, firewalls, IDS, and network equipment within its environment.
- SecureWorks' SIEM Service functions like an extension of PG&E's information security team in a co-managed arrangement whereby SecureWorks' operatives perform the 24x7 monitoring, but in the event of an incident PG&E retains much of the responsibility for remediation with unlimited assistance from SecureWorks.
- Prior to engaging in SIEM, PG&E's information protection group was mainly concerned with policy development. Although monitoring was in place for some systems, there was no comprehensive enterprise level view of security monitoring. PG&E had no visibility into any low profile, multi-system attack. Monitoring was done from a purely operational, non-

security perspective; staff was not looking at security events as much as focusing on operational events such as whether servers were up or down.

- Recognizing the security gaps in the organization, PG&E transformed its information protection group into an information security group and expanded the group's personnel and responsibilities. The group set out to implement a comprehensive, enterprise-level security monitoring program, evaluating the options of (1) expanding its current service with existing providers, (2) developing an in-house security operations center, and (3) opening up the project to market leaders in the information security space. This evaluation led to its decision to implement SecureWorks' SIEM Service.

- Even though it maintains a fully staffed information security group, PG&E estimates that SecureWorks' SIEM Service has saved it from having to recruit, train, and develop between 14 and 16 personnel to staff a 24x7 in-house security operations center (SOC). PG&E also says that matching the level of expertise of the SecureWorks' SOCs with SANS GSEC-certified personnel would be difficult and expensive for PG&E in the context of the Bay Area labor market.

- PG&E's information security team found that the level of tracking, reporting, and support provided by SecureWorks' SIEM Service through the SecureWorks portal "has been the differentiator" for them in benchmarking performance and gaining credibility within their own organization to demonstrate the efficacy of PG&E's information security program.

- The external and internal visibility provided by SecureWorks' SIEM Service has enabled PG&E to create defined response plans in the event of a security breach and practice vulnerability management that prioritizes the allocation of limited resources to fixing the things that are most important.

- Reporting provided by SecureWorks' SIEM Service also contributed to PG&E's successful INFOSEC Assurance-Capability Maturity Model audit by the NSA.

- PG&E highlighted the level of service it received from SecureWorks, noting that two days into the two-week time-frame for implementation, SecureWorks had already started giving PG&E useful alerts.

TEI Framework

Introduction

From the information provided in the in-depth interviews, Forrester constructed a TEI framework for organizations considering implementing SecureWorks' SIEM Service that identifies the cost, benefit, flexibility, and risk factors that affect the investment decision.

Framework Assumptions

Table 2 lists the discount rate used in the PV and NPV calculations and the time horizon used for the financial modeling.

Table 2: General Assumptions

General assumptions	Value
Discount rate	10%
Length of analysis	Three years

Source: Forrester Research, Inc.

Costs

The key cost categories associated with SecureWorks' SIEM Service are: 1) service fees for security event monitoring for all firewalls and intrusion detection devices, servers, and routers; 2) internal account maintenance and administration costs; and 3) pre-planning and development costs.

The project is measured on a three-year basis. The following are the cost inputs to the financial analysis.

SecureWorks' SIEM Service Fees

PG&E engaged SecureWorks' SIEM Service at the Monitored Service Level for $95,000 per month, or $1.14 million annually, at the standard monthly rate of $100 per server.

SecureWorks' Account Maintenance and Administration Costs

PG&E's information security manager estimates the fees for general account maintenance and administration of the SecureWorks relationship at about 0.2 of an FTE per year. At a fully burdened annual compensation of $130,000, this translates into an internal labor cost of $ 26,000 per year.

Pre-Planning and Development Costs

PG&E estimates the internal pre-planning and development effort to implement SecureWorks' SIEM Service as a man-month's worth of effort. At the fully burdened annual compensation of $130,000, this translates into an initial cost of $10,400.

Total Costs

Table 3 summarizes all costs associated with PG&E's implementation of SecureWorks' SIEM Service.

Table 3: Total Costs

Costs	Initial	Year 1	Year 2	Year 3	Total
SecureWorks' SIEM Service fees – Monitoring level		$1,140,000	$1,140,000	$1,140,000	$3,420,000
Account maintenance and administrative costs		$26,000	$26,000	$26,000	$78,000
Internal pre-planning and development	$10,400				$10,400
Total	$10,400	$1,166,000	$1,166,000	$1,166,000	$3,508,400

Source: Forrester Research, Inc.

Benefits

According to PG&E, the main benefit of using SecureWorks' SIEM Service has been to implement a robust information security program with a comprehensive, enterprise-wide view of security monitoring at a lower cost than the alternative of maintaining an in-house SOC and SIEM infrastructure.

- **Cost savings.** Based on total cost of ownership, PG&E evaluated the option of an in-house security information monitoring team and infrastructure and realized that, cost-wise, establishing and maintaining this in-house capability was not as attractive as outsourcing the service. PG&E estimates that it has saved $3.5 million in software and hardware that would have been required for the acquisition and deployment of an enterprise-level SIEM product. In addition, PG&E estimates cost savings of $400,000 in annual maintenance. Another advantage noted by PG&E is that SecureWorks' SIEM Service is an operational expense, not a capital cost. "We're not stuck with a $3.5 million hardware/software investment if it doesn't work out," observed PG&E's information security manager.

  PG&E also estimates that just one fully staffed 24x7 security operations center would need between 14 and 16 personnel. Using SecureWorks' SIEM Service has thus saved the company $1.6 million annually in labor costs. "We manage a contract as opposed to managing a huge staff," said PG&E INFOSEC manager Seth Bromberger, who also noted that with an in-house SOC team the company would have to deal with "issues such as staff attrition, coverage requirements when people are sick, and the ability to maintain a high level of visibility on a lot of data, the majority of which is not important."

  Reduced risk from losses. The risk of loss from external and internal incidents is extremely significant, as evidenced by a regular stream of high-profile cases. SecureWorks' SIEM Service reduces this risk by providing the expert services described above. Forrester's conservative estimate of the benefit to an organization like PG&E of lowering the risk of security loss with a SIEM service is $300,000 annually.

Security Software and Hardware Cost Avoidance

PG&E stated that in order to implement the approximate level of functionality SecureWorks' SIEM Service provides it would need to purchase $3.5 million worth of SIEM software and hardware with which to build an in-house solution. Forrester estimates the software cost at $2,000,000. Hardware and database server software add $1,500,000 for a total benefit in avoided cost of $3,500,000. PG&E estimates that maintenance of this in-house SIEM solution would add 20% to the software costs, or $400,000 annually.

Table 4: Software and Hardware Costs Avoided

Ref.	Metric	Calculation	Year 1	Year 2	Year 3	Total
A1	Investment saved on cost of in-house SIEM solution – software		2,000,000			
A2	Investment saved on cost of in-house SIEM solution – hardware		1,500,000			
At	Total in-house SIEM solution	A1 + A2	3,500,000			
Ato	Total		$3,500,000	$0	$0	$3,500,000

Source: Forrester Research, Inc.

Table 5: Annual Maintenance Costs Avoided

Ref.	Metric	Calculation	Year 1	Year 2	Year 3	Total
A1	Cost of SIEM solution software		2,000,000			
A2	Percent maintenance		20%			
At	Investment saved on annual maintenance for in-house SIEM solution	A1*A2	400,000			
Ato	Total (original)		$400,000	$400,000	$400,000	$1,200,000

Source: Forrester Research, Inc.

In-House Security Operation Center Cost Avoidance

PG&E estimates that it would need between 14 and 16 personnel to perform the same work as a 24x7 SOC. PG&E also noted that the security services provided by SecureWorks currently include three redundant security operation centers, and that approximating that level of service, with the added difficulty of recruiting qualified personnel in the California area, would be challenging. For purposes of this analysis, Forrester conservatively estimates costs avoided for labor at one 24x7 SOC. At a fully burdened annual compensation of $100,000 per person for in-house SOC personnel, this results in cost savings of $1,600,000 per year.

Table 6: In-House SOC Costs Avoided

Ref.	Metric	Calculation	Per Period	Year 2	Year 3	Total
A1	Number of personnel (saved)		16			
A2	Yearly rate per person		100,000			
At	Cost savings in headcount for 24x7 in-house SOC	A1*A2	1,600,000			
Ato	Total		$1,600,000	$1,600,000	$1,600,000	$4,800,000

Source: Forrester Research, Inc.

Lowering The Risk Of Loss From Security Breaches

The generally accepted method of valuing the risk of losses from external and internal incidents is to look at an amount of a potential loss, assume a frequency of loss, and estimate a probability for incurring the loss. Forrester conservatively estimates that this client could face a $10 million loss annually, a figure that includes not only the cost of information loss and brand equity, but also the time required by the company's staff to remediate the issue and get systems fully operational again. Further assuming the probability of a loss of that amount to be 3%, the resulting avoided cost is $300,000 annually, as shown in Table 8. Users of this study are encouraged to use this method with their own assumptions for potential penalty amounts, frequency, and probability. A more comprehensive, expanded method for making this calculation using ranges of probabilities and exposures is described in the Risk section below.

Table 8: Lower Risk of Security Loss

Ref.	Metric	Calculation	Per Period	Year 2	Year 3	Total
A1	Potential exposure - most likely		10,000,000			
A2	Reduced probability of loss		3%			
At	Reduced risk of loss from security breach	A1*A2	300,000			
Ato	Total		$300,000	$300,000	$300,000	$900,000

Source: Forrester Research, Inc.: Total Benefits

PG&E's expected total quantified benefits from SecureWorks' SIEM Service are summarized in the table below.

Table 9: Internal Development Fees Avoided

Benefits	Initial	Year 1	Year 2	Year 3	Total
Investment saved on cost of in-house SIEM solution - software		2,000,000			2,000,000
Investment saved on cost of in-house SIEM solution - hardware		1,500,000			1,500,000

Annual maintenance for in-house SIEM solution		400,000	400,000	400,000	1,200,000
Cost savings in headcount for 24x7 in-house SOC		1,600,000	1,600,000	1,600,000	4,800,000
Reduced risk of loss from security breach		300,000	300,000	300,000	900,000
Total		$5,800,000	$2,300,000	$2,300,000	$10,400,000

Source: Forrester Research, Inc.

Additional Benefits Not Quantified

> *"From a non-technical perspective, this is all about increasing credibility and showing not only executive management but our clients that we're committed to doing the right thing, and we're doing the right thing as far as security is concerned."* – PG&E Information Security Manager

PG&E identified the following benefits of using SecureWorks' SIEM Service, but was not able to quantify these benefits at this time.

Performance Tracking and Audit

PG&E noted that the SecureWorks' SIEM Service portal and SecureWorks' quarterly Trusted Advisor Reports (the SecureWorks' team's review and presentation of customers' security stance and progress) provide a means for closely tracking information security metrics. The information security team can assess system performance on a yearly, quarterly, weekly, daily, and even minute-by-minute basis. The portal also provides a tracking system for incident reporting and response. Data is also available for comparing an organization's security stance with a general average of the security stances of other SecureWorks' customers. This has enabled the team to benchmark PG&E's performance and report this information up to the director of information security and compliance, the CIO, and the executive leadership team. PG&E's information security manager has noted how integral this reporting is to building credibility within the organization. "We had x number of medium severity alerts this past quarter and we met our SLAs on each one of them," he explained. "We could show the history of the ticket with the timestamps for each response." PG&E could track progress on incidents and close out any longstanding audit issues.

Tracking was an important requirement during the course of PG&E's INFOSEC Assurance-CMM audit by the NSA. The ability of SecureWorks' SIEM Service and portal to show auditors that tools with corresponding documentation were integrated into information security processes of vulnerability and risk assessment was a win for the PG&E information security team.

Consistent Access to Skills

SecureWorks' three redundant security operating centers and Threat Intelligence Group provide PG&E with consistent access to the skills needed to maintain the level of service the organization requires for enterprise-level monitoring. PG&E's INFOSEC manager noted that maintaining these personnel in-house would be expensive not only in terms of overall compensation, but also with respect to the added cost of effort occasioned by staff attrition and coverage requirements for unavailable staff. The service level agreements with SecureWorks are a further assurance of consistency of service for PG&E.

The INFOSEC manager also spoke of the difficulty of automation and value of PG&E's access to the deep expertise of SecureWorks' staff through the SIEM Service. "A lot of this still can't be automated," he noted. "A lot of it still needs human intelligence looking at the data in order to provide the quality service we're looking for."

Internal Development Cost Avoidance

Another area of savings for PG&E was in the development of interfaces for security devices. PG&E has a number of mainframes and legacy systems that would need custom interfaces if they were added to an in-house SIEM solution. Because SecureWorks will develop interfaces at no additional cost to the standard monthly service fee, PG&E saves the internal engineering cost of writing interfaces for these systems.

Risk

Risk, the third major component of the TEI model, is used as a filter to capture the uncertainty surrounding different cost and benefit estimates. If a risk-adjusted ROI demonstrates a compelling business case, it raises confidence that the investment is likely to succeed because the risks that threaten the project have been considered and quantified. The risk-adjusted numbers are the "pressure-tested" expectations. In general, risks affect costs by raising the original estimates, and affect benefits by reducing the original estimates.

For the purpose of this analysis, Forrester risk-adjusts cost and benefit estimates to better reflect the level of uncertainty associated with each estimate. The variability is captured as part of this study. The TEI model uses a triangular distribution method to calculate risk-adjusted values. To construct the distribution, it is necessary to first estimate the low, most likely, and high values within the current environment. The risk-adjusted value is the mean of these points.

For example, in the benefit case of investment saved in fielding an in-house 24x7 security operations center, Forrester believes that the number of required staff ranges from 14 to 17, 16 being the most likely number. This range provides the low, high, and most likely values, respectively. Forrester then creates a triangular distribution to reflect the range of expected costs and computes the expected mean. Forrester applies this mean to the fully loaded annual compensation cost of $1,600,000 to arrive at a risk-adjusted value of $1,566,667 per year, or $4,700,000 over three years.

This method has the effect of decreasing the benefit estimates to take into account the fact that original benefit estimates are more likely to be revised downward than upward. The opposite effect is observed for costs; risk adjustments for costs increase the original cost estimates, resulting in a conservative filter for financial assumptions.

The following risks specific to the rollout of SecureWorks' SIEM Service were considered in this study:

- **Software risk.** Forrester risk-adjusted for uncertainty in software estimates. This subsequently affects computations for software maintenance.
- **Labor risk.** Forrester risk-adjusted for uncertainty in labor estimates.
- **Security risk.** Forrester risk-adjusted for uncertainty in the probability and magnitude of security breaches.

Costs

In this case, Forrester does not risk-adjust the cost assumptions. This is done: a) for clarity; b) because the nature, scope, and magnitude of these costs are relatively simple to assess prior to an upgrade initiative; and c) because the precise costs can be set contractually prior to project engagement.

Benefits

Forrester risk-adjusts the benefit estimates to better reflect the level of uncertainty that exists for each estimate.

Security Software and Percentage Maintenance Cost Avoidance

Forrester assumes a level of uncertainty in benefits estimated for the SIEM solution software. The low, most likely, and high estimates for this software are $1,500,000, $2,000,000, and $2,200,000, respectively. The risk-adjusted value is the average of these, or $1,900,000.

The benefit estimates for annual maintenance of the in-house SIEM solution, which are based on a percentage of software costs, are adjusted accordingly, yielding a risk-adjusted value for maintenance of $380,000 annually. These calculations are listed in the tables below.

Table 11: Risk Adjustment — Investment Saved on Software

Ref.	Metric	Calculation	Per Period	Year 2	Year 3	Total
	Variable Low		1,500,000			
A1	Total in-house SIEM solution - software		2,000,000			
	Variable High		2,200,000			
At	Investment saved on cost of in-house SIEM solution - software	A1	2,000,000			
Atr	Total (risk adjusted)		$1,900,000	$0	$0	$1,900,000

Source: Forrester Research, Inc.

Table 12: Risk Adjustment — Investment Saved on Annual Maintenance

Ref.	Metric	Calculation	Per Period	Year 2	Year 3	Total
	Variable Low		1,500,000			
A1	Cost of SIEM solution software		2,000,000			
	Variable High		2,200,000			
A2	Percent maintenance		20%			
	Equation Low	10%*A1	300,000			
At	Annual maintenance for in-house SIEM solution	20%*A1	400,000			
	Equation High	25%*A1	440,000			
Atr	Total (risk adjusted)		$380,000	$380,000	$380,000	$1,140,000

Source: Forrester Research, Inc.

In-House SOC Cost Avoidance

The low, most likely, and high estimates for the internal labor costs that would be required to maintain a 24x7 in-house SOC are assumed to be 14, 16, and 17 FTEs, respectively. These assumptions are multiplied by the $100,000 fully-loaded annual compensation cost. The risk-adjusted value is the average of these, or $1,566,667 per year. The calculations are shown in Table 13 below.

Table 13: Risk Adjustment — Cost Savings for In-house SOC

Ref.	Metric	Calculation	Per Period	Year 2	Year 3	Total
Al	*Variable Low*		14			
A1	Number of personnel (saved)		16			
Ah	*Variable High*		17			
A2	Yearly rate per person		100,000.00			
	Equation Low	Al*A2	1,400,000			
At	Cost savings in headcount for 24x7 in-house SOC	A1*A2	1,600,000			
	Equation High	Ah*A2	1,700,000			
Atr	Total (risk adjusted)		$1,566,667	$1,566,667	$1,566,667	$4,700,000

Source: Forrester Research, Inc.

Lower Risk from Security Breaches

Forrester conservatively estimates that this client could face a $10 million loss annually. Further assuming that SecureWorks' SIEM Service reduces the probability of a loss of that amount by 3%, the resulting avoided cost amount equals $300,000 annually. Expanding on this method, Forrester uses a range of probabilities and exposures as shown in Table 14. For the low assumption, Forrester sets the amount of loss at $800,000, with a reduction in the annual likelihood of loss of 10%. On the high side, the customer could face a loss as large as $35 million, but the overall probability of a loss this large is lower and the reduction in that probability is assumed to be 1%. Using the triangular distribution method described above, the risk-adjusted cost avoidance is calculated to be $243,333 annually.

Users of this study are encouraged to use this method with their own assumptions for potential penalty amounts, frequency, and probability.

Table 14: Risk Adjustment — Lower Risk from Security Loss

Ref.	Metric	Calculation	Per Period	Year 2	Year 3	Total
	Potential Exposure - low		800,000			
A1	Potential Exposure - most likely		10,000,000			
	Potential Exposure - high		35,000,000			

	Reduced Probability of Loss - low		10%			
A2	Reduced Probability of Loss		3%			
	Reduced Probability of Loss - high		1%			
Atl	*Equation Low*		80,000			
At	Reduced risk of loss from security breach	A1*A2	300,000			
Ath	*Equation High*		350,000			
Atr	Total (risk adjusted)	Average (Atl, At, Ath)	$243,333	$243,333	$243,333	$730,000

Source: Forrester Research, Inc.

Flexibility

Flexibility, as defined by Forrester's TEI methodology, represents an investment in additional capacity or agility today that can be turned into future business benefits at some additional cost. This provides an organization with the "right" or the ability to engage in future initiatives, but not the obligation to do so. In the case of SecureWorks' SIEM Service, there are multiple scenarios in which a client might choose to implement one set of services and decide at a later date to engage additional service levels or custom consulting.

Although data for calculating the value of several flexibility options is insufficient at this time, Forrester identified the following areas that present flexibility options for PG&E that would rest on the existing implementation:

- PG&E can now add servers to its network without worrying about capacity planning. SecureWorks' SIEM Service gives PG&E the option of adding as many servers as needed without the cost of internal effort on the part of PG&E's information security team. With this enterprise standard for monitoring, information security no longer becomes a roadblock for network expansion through additional servers.

- New technology group and/or client systems can also be added to the devices monitored by SecureWorks' SIEM Service, saving these technology groups and/or clients the internal information security monitoring effort they would have needed to put in to match the current level of day-to-day monitoring under the PG&E enterprise standard.

The value of flexibility is unique to each organization, and willingness to measure its value varies from company to company (see Appendix A for additional information regarding the flexibility calculation).

TEI Framework: Summary

Considering the financial framework constructed above, the results of the costs, benefits, risks, and flexibility sections using the representative numbers can be used to determine a return on investment, net present value, and payback period.

Tables 15 and 16 below show the risk-adjusted values, applying the risk adjustment method indicated in the Risks section.

Table 15: Total Risk Adjusted Costs

Costs	Initial	Year 1	Year 2	Year 3	Total	Present Value
SecureWorks' SIEM Service fees - Monitoring level		$1,140,000	$1,140,000	$1,140,000	$3,420,000	$2,835,011
Account maintenance and administrative costs		26,000	26,000	26,000	78,000	64,658
Internal pre-planning and development	10,400				10,400	10,400
Total	$10,400	$1,166,000	$1,166,000	$1,166,000	$3,508,400	$2,910,069

Source: Forrester Research, Inc.

Table 16: Total Risk Adjusted Benefits

Benefits	Initial	Year 1	Year 2	Year 3	Total	Present Value
Investment saved on cost of in-house SIEM solution – software		$1,900,000			$1,900,000	$1,727,273
Investment saved on cost of in-house SIEM solution – hardware		1,500,000			1,500,000	1,363,636
Annual maintenance for in-house SIEM solution		380,000	380,000	380,000	1,140,000	945,004
Cost savings in headcount for 24x7 in-house SOC		1,566,667	1,566,667	1,566,667	4,700,000	3,896,068
Reduced risk of loss from security breach		243,333	243,333	243,333	730,000	605,134
Total		$5,590,000	$2,190,000	$2,190,000	$9,970,000	$8,537,115

Source: Forrester Research, Inc.

It is important to note that values used throughout the TEI Framework are based on in-depth interviews with PG&E by Forrester. Forrester makes no assumptions about the potential return other organizations might realize within their respective environments. Forrester strongly advises that readers use their own estimates within the framework provided in this study to determine the expected financial impact of implementing SecureWorks' SIEM Service.

Study Conclusions

- Based on information collected in interviews with PG&E, Forrester found that organizations can realize benefits from outsourced security event management in the form of lower total cost of support for enterprise monitoring and more consistent access to skills compared with trying to build and maintain this same level of service in-house.

- An outsourced managed security service like SecureWorks' SIEM Service was an integral component of PG&E's overall expansion and development of an information security team that, while having a more in-depth and holistic enterprise-level view of information security, could also concentrate on strategic initiatives like policy-setting, security engineering, vulnerability assessment, and threat management programs.

- The tracking and documentation of SecureWorks' SIEM Service helped PG&E establish the robustness of its information security assurance processes in the IA-CMM audit by the NSA.

- Managing a contract instead of an infrastructure for enterprise security monitoring affords PG&E the flexibility to increase server or system capacity as necessary without incurring information security management issues as a roadblock.

The financial analysis provided in this study illustrates the potential way an organization can evaluate the value proposition of SecureWorks' SIEM Service. Based on information collected in in-depth customer interviews, Forrester calculated a three-year risk-adjusted ROI of 193%. All final estimates are risk-adjusted to incorporate potential uncertainty in the calculation of costs and benefits.

Based on these findings, companies looking to implement SecureWorks' SIEM Service can expect to see cost savings and lower risk of losses due to a security breach. Using the TEI framework, many companies might find the potential for a compelling business case for making the requisite investment.

Table 17: ROI, Original and Risk-Adjusted

Summary Financial Results	Original Estimate	Risk-Adjusted
ROI	206%	193%
Total costs (PV)	$2,910,069	$2,910,069
Total benefits (PV)	$8,901,578	$8,537,115
Total (NPV)	$5,991,508	$5,627,046

Appendix A: Total Economic Impact™ Overview

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

The TEI methodology consists of four components to evaluate investment value: benefits, costs, risks, and flexibility. For the purpose of this analysis, the impact of flexibility was not quantified.

Benefits

Benefits represent the value delivered to the user organization — IT and/or business units — by the proposed product or project. Often product or project justification exercises focus just on IT cost and cost reduction, leaving little room to analyze the effect of the technology on the entire organization. The TEI methodology and the resulting financial model place equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization. Calculation of benefit estimates involves a clear dialogue with the user organization to understand the specific value that is created. In addition, Forrester also requires that there be a clear line of accountability established between the measurement and justification of benefit estimates after the project has been completed. This ensures that benefit estimates tie back directly to the bottom line.

Costs

Costs represent the investment necessary to capture the value, or benefits, of the proposed project. IT or the business units may incur costs in the forms of fully burdened labor, subcontractors, or materials. Costs consider all the investments and expenses necessary to deliver the proposed value. In addition, the cost category within TEI captures any incremental costs over the existing environment for ongoing costs associated with the solution. All costs must be tied to the benefits that are created.

Risk

Risk measures the uncertainty of benefit and cost estimates contained within the investment. Uncertainty is measured in two ways: the likelihood that the cost and benefit estimates will meet the original projections and the likelihood that the estimates will be measured and tracked over time. TEI applies a probability density function known as "triangular distribution" to the values entered. At a minimum, three values are calculated to estimate the underlying range around each cost and benefit.

Flexibility

Within the TEI methodology, direct benefits represent one part of the investment value. While direct benefits can typically be the primary way to justify a project, Forrester believes that organizations should be able to measure the strategic value of an investment. Flexibility represents the value that can be obtained for some future additional investment building on top of the initial investment already made. For instance, an investment in an enterprisewide upgrade of an office productivity suite can potentially increase standardization (to increase efficiency) and reduce licensing costs. However, an embedded collaboration feature may translate to greater worker productivity if activated. The collaboration can only be used with additional investment in training at some future point in time. However, having the ability to capture that benefit has a present value that can be estimated. The flexibility component of TEI captures that value.

Appendix B: Glossary

Discount rate: The interest rate used in cash flow analysis to take into account the time value of money. Although the Federal Reserve Bank sets a discount rate, companies often set a discount rate based on their business and investment environment. Forrester assumes a yearly discount rate of 10% for this analysis. Organizations typically use discount rates between 8% and 16% based on their current environment. Readers are urged to consult their organization to determine the most appropriate discount rate to use in their own environment.

Net present value (NPV): The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made, unless other projects have higher NPVs.

Present value (PV): The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total net present value of cash flows.

Payback period: The breakeven point for an investment. The point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Return on investment (ROI): A measure of a project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits minus costs) by costs.

A Note On Cash Flow Tables

The following is a note on the cash flow tables used in this study (see the Example Table below). The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1. Those costs are not discounted. All other cash flows in Years 1 through 3 are discounted using the discount rate shown in Table 2 at the end of the year. Present value (PV) calculations are calculated for each total cost and benefit estimate. Net present value (NPV) calculations are not calculated until the summary tables and are the sum of the initial investment and the discounted cash flows in each year.

Example Table

Ref.	Category	Calculation	Initial cost	Year 1	Year 2	Year 3	Total

Source: Forrester Research, Inc.

Appendix C: About The Consultants

Michelle Salazar
Consultant

Michelle Salazar is a consultant with Forrester's Total Economic Impact (TEI) consulting practice. The TEI methodology focuses on measuring and communicating the value of IT and business decisions and solutions as well as providing an ROI business case based on the costs, benefits, risks, and flexibility of investments.

Prior to joining Forrester, Michelle held leadership roles in operations, technology, and marketing in such large organizations as Shell Corporation and Avaya, Inc. At Shell, she was a product manager for LPG retail distribution initiatives as well as project lead for quality and information security at Shell Philippines. While working at Avaya, she led the inventory reduction program and consulted on various aftermarket operations projects. Michelle also came to Forrester with process improvement and account management experience in high growth start-ups in media and digital services.

Michelle holds a BS in Industrial Engineering from the University of the Philippines and an MBA from the MIT Sloan School of Management.

Jeffrey North
Senior Consultant

Jeffrey North is a senior consultant with Forrester's Total Economic Impact (TEI) consulting practice.

Jeff came to Forrester with consulting and operating experience, notably working with fast-growth companies. He was a founding member of the digital strategy practice at Cambridge Technology Partners, where he specialized in business-value justification for technology investments and client advocacy. As a director in the international and catalog business units at Staples, Jeff built and managed metrics and reporting programs in North America and Europe as the company experienced significant growth. He has also consulted in a business-IT capacity with retailers and life sciences companies.

Jeff holds a BA from St. Lawrence University and an MBA with a concentration in international management and finance from Thunderbird, the Garvin School of International Management.