The Total Economic Impact™ (TEI) of Entrust TruePass and Token-Based Authentication

Project Directors:
Jon Erickson, Senior Industry Analyst
Jan Sundgren, Industry Analyst
Steve Hunt, Vice President

August 2002

Giga Information Group
139 Main St., 5th Floor
Cambridge, Mass. 02142

Tel: (617) 577-4900
Fax: (617) 577-4901

Note: Although great care has been taken to ensure the accuracy and completeness of this report, Giga Information Group is unable to accept any legal responsibility for any actions taken on the basis of the information contained herein.

Circulation or disclosure in whole or in part of this report outside the authorized recipient organization is expressly forbidden without the prior written permission of Giga Information Group.

© 2002 Giga Information Group, Inc. Copying in whole or in part of this report is prohibited without the prior written permission of Giga Information Group.

Table of Contents

Executive Summary **3**
Benefits 3
Costs 4
Risk 5
Flexibility 5
Results 5
Total Economic Impact™ (TEI) Primer **7**
Benefits 7
Costs 8
Flexibility 8
Risk 9
High Volume Web Portal (Scenario A) **10**
Underlying Assumptions 10
Determining Benefits 10
Determining Costs 13
Determining Flexibility 14
Determining Risks 15
Enterprise (Scenario B) **17**
Determining Benefits 17
Determining Costs 19
Determining Flexibility 20
Determining Risks 21
Flexibility 21
High Value Web Portal (Scenario C) **22**
Determining Benefits 22
Determining Costs 24
Determining Risks 24
Flexibility 24
Findings and Recommendations **26**
Appendix A **27**
Appendix B **28**

Executive Summary

Giga employed its Total Economic Impact™ (TEI) methodology to compare two types of strong authentication solutions: one two-factor authentication using token-based technology and one from Entrust Inc. using its Entrust TruePass product. In the case of tokens, a common solution was offered, while with Entrust TruePass, different solutions were included, from roaming-based authentication to true two-factor authentication through the use of smart card technology. Three scenarios were considered, examining the potential impact of each technology on different security environments and vertical industries. The first scenario examined the impact of each of the two types of technologies, token-based authentication and roaming password authentication, on a financial services firm with 50,000 customers engaged in online account access. The second scenario examined the impact of Entrust TruePass and token authentication technology on 10,000 non-roaming internal users accessing a human resources (HR) application. The third scenario examined the impact of these two technologies on a health provider environment requiring high availability and the strongest level of authentication. The three different scenarios are defined in Table 1.

Table 1: Scenarios and Permutations Modeled

Scenario	Elements	How Modeled
High Volume Web Portal — Strong authentication applied to primarily external customers	• Entrust TruePass • Token-based authentication	50,000 customers in a roaming environment
Enterprise — Strong authentication applied to an internal HR application	• Entrust TruePass • Token-based authentication	10,000 internal employees accessing information
High Value Web Portal — True two-factor authentication required to protect trade secrets	• Entrust TruePass • Token-based authentication	10,000 in both an external and internal environment

Source: Giga Information Group

TEI considers four components — cost, benefits, flexibility and risk. In modeling the three different scenarios, and in order to provide an analysis with the highest degree of relevancy, only near-term value was considered during a 36-month investment window.

Benefits

Benefits were derived by first considering areas where information security is generally employed and counteracting potential threats from ineffective security. TEI requires benefits to be traceable to corporate strategy through one or more critical success factors (CSFs), so several CSFs were derived for each scenario. CSFs were derived by researching the Web sites of companies similar to those being modeled. Benefits are summarized in Table 2.

Table 2: Summary of Benefits

Scenario	Benefit	Critical Success Factor Addressed
High Volume Web Portal	Loss liability — protection from civil lawsuit	Reduce costs
	Loss liability — protection of corporate reputation	Reduce costs
Enterprise	Protection of trade secrets	Sustain profitable growth
	Protection of sensitive employee data	Reduce costs
	Protection of sensitive client/vendor data	Sustain profitable growth
High Value Web Portal	Protection of corporate information	Reduce costs
	Protection of external interactions	Sustain profitable growth

Maintain constant access	Reduce costs
End-to-end encryption	Reduce costs

Source: Giga Information Group

Benefits of the application of security are generally considered indirect and are, therefore, the subject of many debates. In modeling benefits for this study, the following factors were considered:

- Companies already have a level of active security commensurate with their respective tolerance levels for risk (based on historic operations).
- Additional security needs are being driven and accelerated by the implementation of increasingly higher levels of interconnectivity (the Internet):
    - Employees working from home/mobile
    - E-commerce/e-business initiatives
    - Web-enabling and/or Web-migrating legacy applications
- Only conceivably likely scenarios for risk abatement were considered (several potential benefits have not been included or quantified).
- Low probabilities of occurrence were used, to properly represent current security practices.

Although some may argue that security is a necessary layer for transactions over the Internet/intranet, the fact remains that companies are free to operate with any level of security they see fit — even fully open and no security. The primary consideration is the company's perception of risk as well as its tolerance for risk. The benefits derived and used in this model represent an attempt at quantifying a typical company's view of prudent behavior.

Primary benefits contained within this report are based on the probability that loss may be avoided at some point in the future. Benefits were determined using the following equation:

$$B = PO * C$$

Where B is Benefit, PO is probability of occurrence of a security breach, and C is the consequence of the breach.

Constructing the probability around a given loss, while arbitrary, allows us to calculate an expected value of the impact of different security strengths on a given environment. In order to construct these values, we relied on a variety of different sources, both based on our internal experience as well as external studies on potential threats and the likelihood that those threats would occur. A sampling of the studies used is referenced in Appendix A.

It is also important to note that one of the primary objectives of this study is to illustrate the process of constructing value statements for security. Estimates contained within the study are based upon a statistically small sampling size and should not be used for across the board validation of one technology compared to another. Each organization must determine its own threshold for risk as well as the value lost as a result of ineffective security in determining which solution is most effective in meeting its security needs. Giga Information Group makes no assumptions that the findings contained within this report will be reproduced in other environments. Organizations should use the model provided to apply the results, based on their own unique circumstances.

Costs

Costs were collected from several sources. Entrust provided standard list pricing for product suites typically proposed under each of the scenarios, including annual maintenance. Entrust also provided recommended hardware lists, typical installation costs and typical full-time equivalents (FTEs) permanently allocated to servicing the security infrastructure. With the exception of the hardware recommendations and list pricing of the product suite, all other input from Entrust concerning the cost of owning/operating the Entrust TruePass product suite was validated by speaking with several representative Entrust customers.

Costs for token two-factor authentication were estimated from standard list prices of token-based technology, with common discounts added as per the current customer base. Cost estimates were validated from internal sources based on customer experiences. Giga assumed a 10 percent loss/failure rate of tokens, which is incorporated into the overall hardware cost of token authentication.

In addition, Giga did not factor into the model the cost of having to renew the tokens after three years, as the benefits arising from that renewal are not considered as part of this report. The Entrust TruePass solution does not require a similar investment in infrastructure costs to realize further benefits past the current investment window. Giga chose not to model this additional cost directly into the financial calculations, as the benefits arising from those additional benefits would need to be modeled as well. The ability, however, to model benefits past four years out is extremely difficult to measure with any degree of accuracy. However, Giga feels that organizations need to take into account the significant additional infrastructure costs on the horizon.

For further information on the costs associated with the deployment of Entrust TruePass and token authentication, please see Appendix B.

Risk

Generally, risk is modeled by considering all possible risks to the benefits as well as the costs. Risks typically include organizational inertia, vendor risk, risk of project cancellation, poor project management, technology risks, etc. For the purposes of this study, normal project risks were considered equal for both technologies, and only risks created by the actual technology were quantified.

Flexibility

Flexibility is defined as the potential value that can be realized into the future as a result of the purchase of the technology solution. Flexibility was examined in each of the three scenarios being considered and where there was quantifiable metrics to calculate, the value of flexibility was included as part of the overall value to the report. In cases where quantitative data was not readily accessible, potential areas were cited to allow readers to consider potential areas where the value of flexibility can be shown.

Results

Table 3 and Table 4 show the results of the TEI analysis. Both standard ROI as well as risk-adjusted ROI are shown. Risk-adjusted ROIs are not representative of a typical project, since standard project risks were not modeled.

Table 3: Financial Results — Entrust TruePass

Entrust TruePass	Scenario A	Scenario B	Scenario C
ROI	124%	150%	421%
Risk-adjusted ROI	68%	106%	335%

Source: Giga Information Group

Table 4: Financial Results — Token-Based Authentication

Token-Based Authentication	Scenario A	Scenario B	Scenario C
ROI	45%	75%	380%
Risk-adjusted ROI	18%	41%	299%

Source: Giga Information Group

Measuring the impact of security has always been an issue of variability. As with measurement of system downtime, estimates are highly variable and unique to each organization. As a result, the objective of this report is to illustrate how to examine the impact of security on a given environment, rather than to project that the financial returns cited

here can be applied to a large population of users. That being said, there are several general assumptions around the three scenarios cited here:

- The returns resulting from security are dependent on the specific potential of exposure and the cost associated with the loss of effective security around sensitive information.
- Based on the assumptions provided for each scenario, Entrust's TruePass product delivered a positive return in each of the three environments.
- Token-based authentication delivered a positive return in all of the three scenarios. Cases where the return was lower than the Entrust TruePass product were a result of primarily higher hardware costs associated with the purchase of the physical token.
- The Entrust TruePass solution provided more options for balancing security against scalability and cost control, by allowing different user groups to access the same technology at different levels of authentication.
- The Entrust TruePass solution delivered a better ROI vs. token-based authentication across all three scenarios considered. It should be noted, however, that for organizations examining their own strong authentication deployment, the results cited here might not translate, due to unique circumstances.

In all three scenarios, the primary value of investing in security was the ability to provide an adequate level of protection based entirely on the value lost from inefficient security. If the potential exposure is greater, it follows that the need for a more secure and, in most cases, a more costly secure environment is needed. This fact is illustrated by looking not only across the different environments, but also between the different types of technologies that are used. Token-based authentication was modeled across the three different environments using roughly the same level of protection across each. Entrust's TruePass product, however, varied the level of protection to reflect the value of exposure. As a result, the cost difference between the two types of technologies did play a role in the final financial returns.

In the financial services case, while token-based authentication did provide an added level of security for the given environment, the potential for loss made the returns for the Entrust TruePass roaming more compelling. If the potential for loss was higher, then the cost for added security would have made the case for stronger security in favor of token authentication.

This is shown in the case of the internal HR application, where the value of the potential loss improves the argument for a stronger security platform. The results show essentially that the potential exposure, both in terms of compensatory and punitive damages, would make the case of stronger authentication more compelling.

In the high value portal scenario, the value of having strong security was offset by the added flexibility capabilities of end-to-end encryption that Entrust provides. Without that feature, the choice between Entrust TruePass and token-based authentication would be essentially determined by the cost difference between the two products. We assume that in this case, the level of protection would be the same with Entrust TruePass with smart card technology and token authentication.

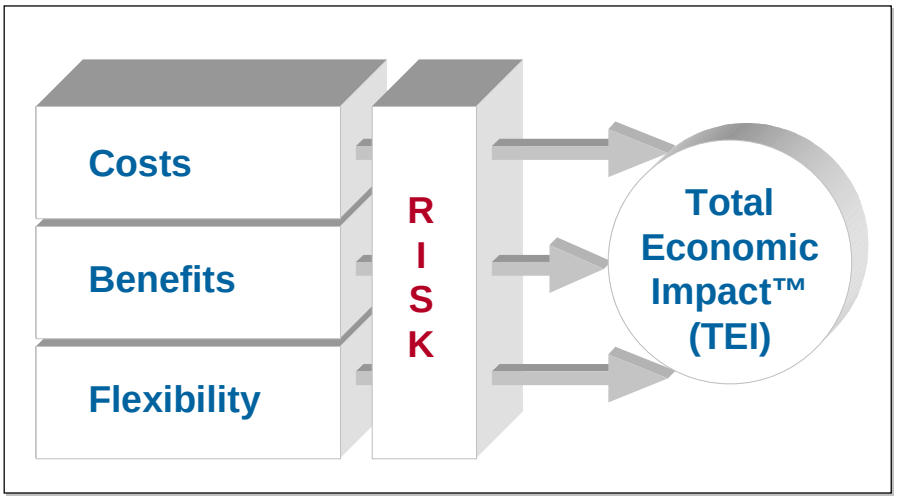
Total Economic Impact™ (TEI) Primer

TEI is primarily a common language tool, designed to capture and properly communicate the value of IT initiatives in a common business language. In so doing, TEI considers four elements of any initiative. Those elements are:

- Benefits
- Costs (sometimes referred to as TCO)
- Flexibility
- Risk

Benefits, flexibility and costs are considered, through the filter of risk assessment, in determining an expected return on investment (ROI) for any given initiative.

TEI Conceptual Diagram



Source: Giga Information Group

Benefits

Benefits represent the value delivered to the business by the proposed project. Oftentimes, IT project justification exercises focus on cost (e.g., TCO) and cost reductions. This, however, is very parochial and single-dimensional thinking. In today's market, many times IT is deployed as an offensive weapon, with greater value expectations than simple cost reduction, especially when those cost reductions tend to focus within IT. TEI captures the value proposition of the proposed project through benefits.

Each benefit captured by TEI must be traceable back to one or more critical success factors (CSFs). These CSFs are, in turn, traceable back to a higher-level business strategy. If the proposed solution has a potential benefit that cannot be linked to a CSF, then it is not a benefit for the organization considering it (it may be a benefit for some other organization, but not this one). Therefore, TEI does not allow value to be generated from that benefit.

Although TEI does allow the consideration of "benefits" in the form of cost reductions within IT, strictly speaking, TEI considers benefits to accrue to the business units. "Benefits" that are considered cost reductions within IT are considered by TEI to accrue as negative TCO to the IT budget, thereby showing a reduced TCO (TCO is considered by TEI to be a single-dimension, cost-centric focus on the IT budget).

TEI starts with a discovery of areas of potential benefit. Quantification of the value of each benefit captured during discovery must be validated by someone who has within his or her span of control the ability to actually capture that benefit. That is, someone cannot arbitrarily assign a value to a benefit if that person is not in a position to actually

deliver that benefit should the project be approved. Ostensibly, projects that are expected to deliver business value require some effort on the part of the business to realize that value. That effort may be in the form of training, organizational change or a large-scale modification of current business processes. Therefore, TEI requires dialog with the actual business leaders who will be responsible for making the necessary changes to capture the proposed benefit, during the justification phase. TEI captures this dialog in the form of the names of the individuals who validated each value number entered against each benefit.

Within TEI, each benefit entered has a specific capture date. Although the benefit may actually be captured over time, TEI requires the estimation of a date when the benefit has been mostly captured. TEI will then place the value delivered in the appropriate time frame within the project.

Costs

Costs represent the investment necessary to capture the value, or benefits, of the proposed project. Costs may either be incurred by IT or by the business units. Costs may be in the form of fully burdened labor, subcontractors or materials. Costs consider all investment and expenses necessary to deliver the value proposed.

Flexibility

Flexibility can be defined in several ways. Generally, as used by TEI, it represents investing in additional capacity that can, for some future additional investment, be turned into business benefit. Take, for instance, an investment in upgrading the current version of word processor across the enterprise. The primary driver for considering the upgrade may be standardization (to increase efficiency) and licensing (to decrease IT costs). However, a collaborative workgroup feature may, indeed, be translated into even more efficiency at a later time when the culture is ready to absorb the discipline necessary to capture that benefit. That collaborative feature does not promise benefit during this phase of the project and must be captured at a later time for additional investment (training). However, just having that option has present value. The flexibility component of TEI captures that value.

Flexibility can also be defined as realizing that for any given project, management has several decision points along the way. At each decision point, management can steer the project to a different outcome or cancel it altogether. Many net present value (NPV) evaluations fail to take this management flexibility into account. Because TEI's flexibility component uses the industry standard Black-Scholes options formula, this management flexibility factor is taken into consideration.

TEI divides a project into one or more phases. The first phase is considered the "benefits" phase — it is the phase expected to deliver the primary benefits. The benefits phase is usually no more than one budget cycle long, and it is the primary reason the project is being considered. All other phases are "options" or "flexibility" phases. For additional investment at some point in the future, business benefit can be captured during these "options" phases.

TEI applies the Black-Scholes options pricing equation to all phases other than the benefits phase. The Black-Scholes equation takes five inputs to calculate a present day value of having flexibility, or options. Those five inputs are:

1. The value, or business benefit, that can be captured should the option be exercised (additional future investment applied to capture the benefit). This value is expressed in present value terms.
2. The time to the decision date beyond which the option or flexibility will expire. Expiration could be due to business changes or technology obsolescence.
3. The cost of the investment to exercise the option (capture the benefit).
4. The risk-free interest rate (typically the interest rate of government securities is used.)
5. The volatility of one's industry or sector. TEI uses the volatility of the stock prices within the company's sector as this input.

Risk

Risks are used to widen the possible outcomes of the project. Because nobody can accurately predict the future, there is inherent risk in any project. TEI captures risk in the form of risks to benefits and risks to costs.

Risks to benefits considers all possible risks to each and every benefit. Risks to costs considers all possible risks to each and every cost. Then, a range is chosen by applying best judgment for each cost and benefit, based on the set of risks assigned to each cost and benefit. The range is entered in the form of a low estimate, a most likely value and a high estimate. For example, the risks to a cost may result in a range from the expected value as the low estimate, to two times the expected value as the high for a particular cost (representing a potential two times cost overrun).

TEI applies a probability density function known as the "triangular distribution" to the entered values. The expected value (mean) of the distribution is used as the risk-adjusted cost or benefit number. The risk-adjusted costs and benefits are then summed to yield a complete risk-adjusted summary and ROI.

Typical project risk factors to be considered include:

- Vendors: The risk that the vendor of a product or technology may need to be replaced at some point during the project duration
- Products: The risk that a product will not deliver the functionality expected
- Architecture: The risk that the current product architecture will not allow future infrastructure decisions and changes
- Culture: The risk that an organization will be unable to absorb the new technology or adapt to its implementation
- Delays: The impact on revenues of a project delay or cancellation
- Size: The direct correlation of project risk to the size of the project, as measured by application size or budget

High Volume Web Portal (Scenario A)

Underlying Assumptions

The high volume Web portal scenario modeled a company based in financial services that employed strong authentication capabilities, primarily to allow its private clients access to their accounts and information related to their accounts.

Table 5 lists several of the underlying assumptions used in the roaming scenario.

Table 5: Assumptions Used in High Volume Web Portal Scenario

Variable	As Modeled
Number of users	50,000
Net present value discount factor	10%
Currency	USD
Person hours in a person year	2,080
System administrator annual salary, fully burdened	$60,000
Cost to customer for an hour's worth of time	$50

Source: Giga Information Group

Determining Benefits

The benefits of a roaming Entrust TruePass solution are based primarily on the avoided cost of a security breach of a customer's personal data. Benefits are defined by TEI as accruing primarily to the business itself, as opposed to cost reductions, which generally accrue to IT. Benefits, therefore, must be relevant to the business. That is, features of solutions that are advertised as benefits can only provide true benefit to a company if those features support an element of the company's strategy.

In the case of the high volume Web portal solution, it is assumed that unauthorized access to a customer's online credentials impacts both the financial institution and the customer directly. For the financial institution, this impact can be seen in two different ways. First, there are costs with having to repair and restore the customer back to the state before the intrusion. In addition, there is potential liability associated with brand value, because recurring attacks might occur.

In addition to potential loss by the financial institution, there are also the potential damages from the customer side. Costs might include the out-of-pocket expenses related to having to resolve the breach of security.

The probability of loss for each of the two technologies was compared to an environment with passwords only.

Loss liability (protection from lost assets) — One of the most immediate cost avoidance benefits as a result of stronger security is protection of a client's assets. In this scenario, we assume that the online tool provides access to user accounts and allows the user to trade and transfer assets both within accounts as well as to external accounts. While most financial intuitions limit their liability through insurance, there is still the potential that unauthorized access could cause the loss of some portion of the client's account. Assuming that this is particularly focused on private client customers, the demand for stronger security is directly linked to the size of the asset base. In order to determine the potential savings from a stronger authentication solution, it is first necessary to examine the probability of unauthorized access using just passwords only. Table 6 illustrates the potential loss using just passwords as a means of authentication.

Table 6: Corporate Exposure With Passwords

		Year 1	Year 2	Year 3
A1.	Average value of account	$ 1,000,000	$ 1,000,000	$ 1,000,000
A2.	Bank liability of account fraud	$ 300,000	$ 300,000	$ 300,000
A3.	Probability of fraud	0.020%	0.020%	0.020%
A4.	number of users	50,000	$ 50,000	$ 50,000
Calc	(A2*A3)*A4	$ 3,000,000	$ 3,000,000	$ 3,000,000

Source: Giga Information Group

For the purpose of this analysis, we assume that the presence of stronger authentication would reduce the size of the loss by reducing the potential that a customer's credentials would be stolen. In roaming mode, Entrust TruePass does not provide two-factor authentication, but it does improve on the security of a typical password system. Entrust TruePass roaming credentials are stored encrypted on the server, and they are not decrypted until they have been downloaded to the client. In addition, organizations typically incorporate a third registration and authentication field into the initial log-on to strengthen the level of authentication. This approach reduces the possibility of credentials being stolen from the server or sniffed as they cross the Internet. Table 7 illustrates the exposure when using Entrust TruePass authentication.

Table 7: Corporate Exposure With Entrust TruePass

		Year 1	Year 2	Year 3
B1	Average value of account	$1,000,000	$1,000,000	$1,000,000
B2	Bank liability of account fraud	$300,000	$300,000	$300,000
B3	Probability of fraud	0.007%	0.007%	0.007%
B4	Number of users	50,000	50,000	50,000
Calc:	(B2*B3)*B4	$1,000,000	$1,000,000	$1,000,000

Source: Giga Information Group

As Table 7 illustrates, while Entrust TruePass does not eliminate the potential loss, it does reduce the potential that an end user's login credentials would be sniffed without the end user's knowledge. Based on the following assumptions, the annual estimated savings from the use of Entrust TruePass is $2,000,000 (i.e., $3,000,000-$1,000,000). During a three-year period of analysis, the savings resulting from the use of Entrust TruePass are estimated to be $4,973,704, assuming the annual discount rate of 10 percent.

With token authentication, the underlying assumptions in terms of size of account and the average value exposed is roughly equivalent. However, we assume that the strength of security exceeds the Entrust TruePass technology in this scenario, because the token technology provides true two-factor authentication: In addition to knowing a password, a user must have the token. As a result, we estimate that the likelihood of unauthorized access decreases to one in 40,000 as a result of the introduction of the token authentication. Table 8 illustrates the estimates used in the analysis.

Table 8: Corporate Exposure With Token Authentication

		Year 1	Year 2	Year 3
C1	Average value of account	$1,000,000	$1,000,000	$1,000,000
C2	Bank liability of account fraud	$300,000	$300,000	$300,000
C3	Probability of fraud	0.003%	0.003%	0.003%
C4	Number of users	50,000	50,000	50,000
Calc:	(C2*C3)*C4	$375,000	$375,000	$375,000

Source: Giga Information Group

In addition to the potential loss of actual assets, there are also costs on the customer side to restore any potential damage that might be incurred as a result of a potential security breach. Table 9 illustrates the assumptions made regarding the cost to restore the customer data with the scenario of using passwords alone:

Table 9: Customer Exposure With Passwords

		Year 1	Year 2	Year 3
A1	Cost of unauthorized intrusion	$10,000	$10,000	$10,000
A2	Number of users	$50,000	$50,000	$50,000
A3	Probability of fraud	0.020%	0.020%	0.020%
Calc:	(A1*A2)*A3	$100,000	$100,000	$100,000

Source: Giga Information Group

As in the benefit above, security is increased as a result of the introduction of stronger authentication from Entrust TruePass. Table 10 illustrates the potential change with the introduction of the Entrust TruePass technology.

Table 10: Customer Exposure With Entrust TruePass

		Year 1	Year 2	Year 3
B1	Cost of unauthorized intrusion	$10,000	$10,000	$10,000
B2	Number of users	50,000	50,000	50,000
B3	Probability of fraud	0.007%	0.007%	0.007%
Calc:	(B1*B2)*B3	$33,333	$33,333	$33,333

Source: Giga Information Group

Based on the following assumptions, the value saved from the Entrust TruePass in terms of end-user costs avoided is estimated to be $66,667 per year to a total three-year NPV discounted savings of $165,790.

Increasing the strength of the security through token authentication further decreases the potential exposure resulting from unauthorized access. Table 11 illustrates the potential change from a password-based environment with the introduction of factor authentication.

Table 11: Customer Exposure With Token Authentication

		Year 1	Year 2	Year 3
C1	Cost of unauthorized intrusion	$10,000	$10,000	$10,000
C2	Number of users	50,000	50,000	50,000
C3	Probability of fraud	0.003%	0.003%	0.003%
Calc:	(C1*C2)*C3	$12,500	$12,500	$12,500

Source: Giga Information Group

Based on the following assumptions, the value saved from the strong authentication in terms of end-user costs avoided is estimated to be $87,500 per year for a total three-year savings of $217,600.

Loss liability (protection of brand) — Recurring attacks have the potential to reduce the confidence around a customer-facing application. Recurring attacks also have the potential of negatively impacting the perception that current users have about the safety of their assets, even though they may not be directly impacted by the intrusion. As a result, the impact of an unauthorized intrusion can have negative repercussions above and beyond those users who are immediately affected. This can be seen in the increase in churn among the current customer base and, as a result, the possibility of loss of current customers based on the perception of ineffective security. Although difficult to estimate, outlining assumptions is a first step in quantification of the estimates. The primary assumptions used are shown in Table 12.

Table 12: Loss From Brand Exposure

		Year 1–Year 3
A1	Average account size	$1,000,000
A2	Profit margin per client	15%
A3	Number of clients who would cancel as a result of repeated attacks	2
A4	Assume one scenario over a three year period	1
Calc:	(A2*A3)*A4	$300,000

Source: Giga Information Group

Based on the following assumptions, the value saved from stronger authentication in terms of potential customer abandonment loss is estimated to be roughly $300,000.

Determining Costs

Costs were determined separately for both the token authentication and Entrust environments. Token authentication costs were derived by first estimating the tasks necessary to install and maintain the solution as well as the additional hardware and software requirements while Entrust costs were provided by Entrust, then validated by speaking with several Entrust customers.

Entrust supplied typical cost estimates for rollout and annual maintenance/administration of its solutions and also recommended product suites and standard pricing and maintenance fees for those product suites. Rollout and annual maintenance/administration costs were validated by contacting several Entrust customers.

The overall costs for the Entrust TruePass and token-based authentication are shown in Table 13. For a further description of the costs quantified, see Appendix B.

Table 13: Costs — Entrust TruePass

	Year 1	Year 2	Year 3
Software	$(739,860)	$(112,860)	$(112,860)
Hardware	$(80,000)	–	–
Internal IT Costs	$(580,972)	$(125,000)	$(125,000)
End User Costs	$(604,167)	$(187,500)	$(187,500)
Total Costs	$(2,004,999)	$(425,360)	$(425,360)

Source: Giga Information Group

Table 14: Costs — Token Authentication

	Year 1	Year 2	Year 3
Software	$(940,416)	$(94,800)	$(94,800)
Hardware	$(1,637,600)	–	–
Internal IT costs	$(1,298,603)	$(380,000)	$(380,000)
End user costs	$(604,167)	$(187,500)	$(187,500)
Total costs	$(4,480,786)	$(662,300)	$(662,300)

Source: Giga Information Group

The primary cost differences between the two solutions are as follows:

- For token authentication, there are added costs for hardware, in terms of additional cost of procuring and the distribution of tokens, which is not included in the Entrust TruePass solution.
- Token authentication requires additional administrative costs to replace lost or stolen tokens.
- It is also important to note that for the purpose of this model, we did not include the additional cost after three years of having to renew the physical tokens for token authentication. Including this cost into the analysis without incorporating the benefits associated with that cost would skew the findings, and as a result, the costs were not included but should be taken into account, as they are a significant cost past the initial investment period.

Determining Flexibility

Flexibility was examined primarily from the standpoint of the ability of the Entrust TruePass solution to provide digital signatures and end-to-end encryption capabilities for specific applications. For the purpose of this scenario, the value of flexibility was modeled specifically from the standpoint of reducing costs for account administration among the private client banking customers. Based on discussions with financial organizations, reducing the cost of paper-based transactions can potentially be seen as a benefit with the introduction of digital signature technology on top of the Entrust TruePass platform. The process of setting up an account can now be accomplished through the use of digital signatures, where before that process was only achievable through paper-based records.

Table 15 illustrates the potential value of digital signatures on top of the base investment. Benefits were modeled on the total time it takes internal employees to process a paper-based document compared to the time it takes to authenticate using digital signature technology. The costs were modeled from the additional cost of having to integrate the digital signature solution into the organization.

Table 15: Option Value From Digital Signatures

Variable	Description	Amount	Value
S	Value of the assets associated with the future adoption of new business tools and methods	$415,706	Dollars
X	Spending required to acquire the assets	$344,100	Dollars
T	Length of time spending can be deferred (expiration)	2	Year(s)
R	Risk-free rate of return	6.50%	Years
σ	Market volatility, per year of potential assets — market-based	0.60	Per year
Black-Scholes Option Price (Value)		$182,408	

The resulting option value, $182,408, is based on the cost and benefit resulting from installing digital signatures at the organization.

Other possible areas of flexibility include:

- Reduced possibility of an internal security breach through the use of end-to-end encryption
- Extending the use of digital signatures to other transaction-based account authentication (i.e., equity trading)

Building a solution around end-to-end encryption that would allow the customer to access related sites while maintaining the same credentials throughout. For example, there is a reduced possibility of an internal security breach of the client's information.

Determining Risks

Risk modeling was limited to only those risks perceived to be created by the choice of technology (as opposed to modeling all normal project risks). The primary risk drivers were as follows:

Token authentication:

- Loss of keys, reducing the likelihood that the token authentication will be used
- Hardware failure (broken token)
- Keyboard sniffing Trojan attack to get personal identification number (PIN)
- Forgot token, can't log into session

Entrust:

- Theft of credentials by gaining access to a user's keys or posing as another user during enrollment. This risk is assumed to have a short window of opportunity, because the intended user is expected to eventually call asking for his or her enrollment.
- Password guessing attack, shoulder surfing attack.

A possible risk for Entrust is the loss of all keys due to a failure of the server or its data storage device. Giga, however, considered any implementation of such a mission-critical solution where the server was not made

redundant and/or reliable tape backups did not exist to be wholly incompetent. The expected probability of occurrence, therefore, was too low to model.

In order to incorporate the risks cited above, the impact of risk was applied to different estimates contained within the model. Risk was applied both to cost and benefit estimates contained within the report.

In the case of costs, we assumed that there is a potential that the costs to initially register might increase, further burdening end users in accessing their financial information. In addition, we assumed an increase in support calls related to the use of the two technologies, because users may not be able to use the self-help features that accompany the technology. Table 16 illustrates an example of the application of risk to the estimate of the time it takes an end user to initially register for either Entrust TruePass or token authentication

Table 16: Risk — User Registration

		Year 1
A1	Minutes to register	10
Low	90%	9
High	140%	14
RA		11
A2	Number of users	50,000
A3	Value per hour — end user	$50.00
Calc:	(A1/60)*A2*A3	$458,333

Source: Giga Information Group

As Table 16 shows, the original value for the time it takes a given end user to log in and initially register is estimated at 10 minutes. Applying a range of possible outcomes to that estimate allows us to compute a risk-adjusted value, leading to an increase in user registration costs from $416,667 to $458,333.

In the case of benefits, we applied risk to the actual exposure that was being considered. In the case of both the Entrust TruePass and token authentication, we reduced the potential liability for the given organization, thereby reducing the overall benefit over time. Table 17 illustrates the risk applied to the exposure of corporate costs for unauthorized access.

Table 17: Risk — Exposure With Passwords

		Year 1	Year 2	Year 3
A1	Average value of account	$1,000,000	$1,000,000	$1,000,000
A2	Bank liability of account fraud	$300,000	$300,000	$300,000
Low	40%	$120,000	$120,000	$120,000
High	110%	$330,000	$330,000	$330,000
RA	Average	$250,000	$250,000	$250,000
A3	Probability of fraud	0.020%	0.020%	0.020%
A4	Number of users	50,000	$50,000	$50,000
Calc:	(A2*A3)*A4	$2,500,000	$2,500,000	$2,500,000

Source: Giga Information Group

Enterprise (Scenario B)

The enterprise scenario modeled companies of various sizes employing Entrust TruePass and strong authentication primarily for internal purposes. In particular, the benefits of Entrust TruePass and strong authentication are modeled on a scenario in which internal users are accessing an internal HR application for information regarding their benefit and compensation plans.

Table 18: Underlying Assumptions in Enterprise Scenario

Variable	As Modeled
Number of users	10,000
Net present value discount factor	10%
Currency	USD
Person hours in a person year	2,080
General user annual salary, fully burdened	$105,000
System administrator annual salary, fully burdened	$75,000

Source: Giga Information Group

Determining Benefits

As with the high volume Web portal scenario, the value of stronger authentication is based on the potential exposure if information is not securely protected. In terms of damages resulting from an unauthorized access to an employee's information, there exists the potential of loss in two separate areas. The first, punitive damages, results from the corporation being found negligent in storing personal information. In addition, there is the potential for compensatory damages arising from ineffective security with an employee's confidential HR records.

The potential in this area exists and has existed, so most companies have good procedures in place to minimize the threat. However, the threat is magnified with companies transitioning to self-serve HR systems using the Web. A perturbation in employee trust can have significant ramifications in the areas of recruiting/retention, quality, customer satisfaction, growth strategies, revenue and costs.

As in the case of roaming, Giga assumed that there is a higher level of protection associated with tokens as compared to the Entrust TruePass solution. Areas of potential exposure arise around both punitive and compensatory damages resulting from ineffective security.

Punitive damages — The damage caused by a loss of confidential employee information can be inflicted through compensatory and punitive penalties imposed on the organization. The assumptions around punitive damages are as follows in an environment with just passwords in place:

Table 19: Exposure With Passwords

		Year 1	Year 2	Year 3
A1	Potential damage of HR Lawsuit	$625,000	$625,000	$625,000
A2	Probability of fraud	0.020%	0.020%	0.020%
A3	Number of users	10,000	10,000	10,000
Calc:	(A2*A3)*A4	$1,250,000	$1,250,000	$1,250,000

Source: Giga Information Group

With both Entrust TruePass and token authentication, the potential of a security breach is reduced, because the likelihood that a password can be appropriated maliciously is reduced. We assume a higher level of security with the token authentication solution, as Table 20 and Table 21 indicate. Though Entrust TruePass in this scenario represents two-factor authentication (the credential is stored locally, so an attacker would need access to the specific PC as well as the password), the probability of a breach is still higher than in the roaming scenario, because the corporate environment entails higher risk: Passwords are stolen more easily and access to specific PCs is not necessarily controlled. As in the previous scenario, the presence of a third authentication field is included around the Entrust TruePass solution. With a token solution, the fact that users generally keep the tokens with them reduces these risks, so the probability remains the same as in the first scenario.

Table 20: Exposure With Entrust TruePass

		Year 1	Year 2	Year 3
B1	Potential damage of HR lawsuit	$625,000	$ 625,000	$625,000
B2	Probability of fraud	0.00833%	0.00833%	0.00833%
B4	Number of users	10,000	10,000	10,000
Calc:	(B2*B3)*B4	$520,833	$520,833	$520,833

Source: Giga Information Group

Table 21: Exposure With Token Authentication

		Year 1	Year 2	Year 3
C2	Potential damage of HR lawsuit	$625,000	$625,000	$625,000
C3	Probability of fraud	0.003%	0.003%	0.003%
C4	Number of users	10,000	10,000	10,000
Calc:	(C2*C3)*C4	$156,250	$156,250	$156,250

Source: Giga Information Group

Based on the assumption between Entrust TruePass and token authentication, the savings resulting from using Entrust TruePass are estimated to be $729,167 per year, or a total net present value of $1,813,330.

With token authentication, the potential savings equates to $1,093,750 per year, or a total net present value of $2,719,994.

Compensatory damages — In addition to punitive damages, there exists the possibility of compensatory damages from unauthorized access of personnel records. Giga assumes that the compensatory damages are to compensate the damaged employee as a result of out-of-pocket expenses resulting from the unauthorized security breach. Table 22 shows the assumptions that are used to derive the potential loss of using just passwords alone.

Table 22: Exposure With Passwords

		Year 1	Year 2	Year 3
A1	End user cost of an unauthorized intrusion	$30,000	$ 30,000	$30,000
A2	Possibility of fraud	0.0200%	0.020%	0.020%
A3	Number of users	10,000	10,000	10,000

Calc:	(A1*A2)*A3	$60,000	$60,000	$60,000

Source: Giga Information Group

As with punitive damages, there is a slightly reduced probability of breach resulting from the use of token authentication as compared to the Entrust TruePass technology. Table 23 shows the assumptions regarding Entrust TruePass.

Table 23: Exposure With Entrust TruePass

		Year 1	Year 2	Year 3
B1	End user cost of an unauthorized intrusion	$30,000	$30,000	$30,000
B2	Possibility of fraud	0.0083%	0.0083%	0.0083%
B3	Number of users	10,000	10,000	10,000
Calc:	(B1*B2)*B3	$25,000	$25,000	$25,000

Source: Giga Information Group

Based on the assumption between Entrust TruePass and token authentication, the savings resulting from using Entrust TruePass are estimated to be $35,000 per year or a total net present value of $87,040.

For token authentication, the assumptions are shown in Table 24.

Table 24: Exposure With Token Authentication

		Year 1	Year 2	Year 3
C1	Cost of unauthorized intrusion	$30,000	$30,000	$30,000
C2	Number of users	$10,000	$10,000	$10,000
C3	Possibility of fraud	0.004%	0.004%	0.004%
Calc:	(C1*C2)*C3	$10,714	$10,714	$10,714

Source: Giga Information Group

With token authentication, the potential savings equate to $49,286 per year, or a total net present value of $122,566.

Determining Costs

Costs were similar as in the roaming scenario. The primary difference between the costs for the roaming and enterprise scenario is that the cost per user was modeled based on the fully burdened salary of an internal user, rather than in the roaming case where the value was based on the value of an external customer's time.

The costs for both solutions are illustrated in Table 25 and Table 26.

Table 25: Costs — Token Authentication

Tokens	Year 1	Year 2	Year 3
Software	$(237,000)	$(47,400)	$(47,400)
Hardware	$(599,200)	–	–
Internal IT costs	$(678,603)	$(76,000)	$ (76,000)

End-user costs	$(120,833)	$(37,500)	$(37,500)
Total costs	$(1,635,637)	$(160,900)	$(160,900)

Source: Giga Information Group

Table 26: Costs — Entrust TruePass

Entrust TruePass	Year 1	Year 2	Year 3
Software	$(319,588)	$(47,988)	$(47,988)
Hardware	$(80,000)	–	–
Internal IT Costs	$(156,918)	$(25,000)	$(25,000)
End User Costs	$(120,833)	$(37,500)	$(37,500)
Total Costs	$(677,339)	$(110,488)	$(110,488)

Determining Flexibility

As in the roaming scenario, flexibility was considered concerning the added capability of the Entrust TruePass suite. Potential areas where flexibility can be seen are as follows:

- Providing employees with the capability of updating their HR records by using digital signature capabilities.
- End-to-end encryption provides additional internal intrusion protection around an employee's encrypted information. This further reduces the potential of an unauthorized potential exposure of employees' private data.
- Integrate seamlessly with other portal technologies, like PMI
- Improve automatic user management in such areas as credential checking, rollover
- Further integrate self-registration and recovery features into the overall solution

This study calculated the value of flexibility as it relates to the use of digital signatures. We are assuming that with digital signatures in place, an organization is able to reduce the cost of having to process internal HR paper documents.

Table 27 illustrates the potential value of digital signatures on top of the base investment. Benefits were modeled on the total time it takes internal employees to process a paper-based document compared to the time it takes to authenticate using digital signature technology. The costs were modeled from the additional cost of having to integrate the digital signature solution into the organization.

Table 27: Potential Value of Digital Signatures on Top of the Base Investment

Variable	Description	Amount	Value
S	Value of the assets associated with the future adoption of new business tools and methods	$184,758	Dollars
X	Spending required to acquire the assets	$150,000	Dollars
T	Length of time spending can be deferred (expiration)	2	Year(s)
R	Risk-free rate of return	6.50%	Years
σ	Market volatility, per year of potential assets —	0.60	Per year

market-based	
Black-Scholes Option Price (Value)	$82,320

Determining Risks

Risks are similar in the enterprise scenario as in the case of the roaming scenario. Similar impacts were applied to the cost and benefit estimates contained within the model.

Flexibility

Flexibility was not modeled for either solution, although several features exist for Entrust that were not modeled as either benefits or flexibility. Such features include:

- Product maturity and installed based
- Ability to detect tampering
- Support for workgroup access to encrypted files

High Value Web Portal (Scenario C)

In the final scenario, we assume a high value web portal environment with strong authentication technology within a health services organization of 10,000 end users. The organization requires the protection of customer records, both for liability as well as for regulatory (i.e., HIPAA) purposes. As a result, the strongest level of authentication was employed both from the Entrust TruePass perspective as well as from token authentication. In the case of Entrust TruePass, we assumed that the organization was using smart card technology to provide the strongest level of two-factor authentication within the environment.

Determining Benefits

As with the other two scenarios, the main security benefits are based primarily on the value of protection and the consequences if that information is not protected. Because this is a regulated environment, there are two primary penalties resulting from accidental access of personnel records.

With the introduction of smart card technology as part of the Entrust TruePass solution, Giga feels that the level of protection is equal to that of token authentication in reference to accidental exposure of patients' records.

Criminal fines — According to HIPAA, there are several criminal penalties resulting from the loss of patients' personal data. The minimum fine is $25,000. In this scenario, the probabilities of breaches for both passwords-only and two-factor authentication are considerably higher than in the other scenarios, because we are assuming non-malicious breaches stemming from the sharing of credentials among workers. The probabilities for two-factor authentication are still lower than for passwords, however, because the sharing of a token or smart card is less likely than the sharing of just a password. The following assumptions were used for cases where just passwords were used:

Table 28: Exposure With Passwords

		Year 1	Year 2	Year 3
A1	Minimum fine	$25,000	$25,000	$25,000
A2	Probability of fraud	0.400%	0.400%	0.400%
A3	Number of users	10,000	10,000	10,000
Calc:	(A2*A3)*A4	$1,000,000	$1,000,000	$1,000,000

Source: Giga Information Group

With the introduction of smart card technology, we assume that the level of protection is equivalent between Entrust TruePass and token authentication in terms of direct benefits.

Table 29: Exposure With Entrust TruePass

		Year 1	Year 2	Year 3
B1	Minimum fine	$25,000	$25,000	$25,000
B2	Probability of fraud	0.02000%	0.02000%	0.02000%
B4	Number of users	10,000	10,000	10,000
Calc:	(B2*B3)*B4	$50,000	$50,000	$50,000

Source: Giga Information Group

Table 30: Exposure With Token Authentication

		Year 1	Year 2	Year 3
C2	Bank liability of account fraud	$25,000	$25,000	$ 25,000
C3	Probability of fraud	0.020%	0.020%	0.020%
C4	Number of users	10,000	$10,000	$10,000
Calc:	(C2*C3)*C4	$ 50,000	$50,000	$50,000

Source: Giga Information Group

The resulting strong security has the potential to reduce the loss resulting from unauthorized access by roughly $950,000 per year, or a total net present value of $2,362,509.

Civil fines — In addition to criminal fines that could be imposed as a result of unauthorized disclosure of patients' data, there exists the potential of various civil fines around the breach of security. Aside from criminal penalties assigned by HIPAA, there is the potential for civil penalties brought about by loss of patients' data. Assume for every 1,000,000 users, there is a civil penalty of $2,400,000 imposed. Table 31, Table 32 and Table 33 outline the assumptions.

Table 31: Exposure With Passwords

		Year 1	Year 2	Year 3
A1	Average potential exposure	$2,400,000	$2,400,000	$2,400,000
A2	Possibility of fraud	0.0100%	0.01000%	0.01000%
A3	Number of users	10,000	10,000	10,000
Calc:	(A1*A2)*A3	$2,400,000	$2,400,000	$2,400,000

Source: Giga Information Group

Table 32: Exposure With Entrust TruePass

		Year 1	Year 2	Year 3
B1	Average potential exposure	$2,400,000	$2,400,000	$2,400,000
B2	Possibility of fraud	0.0001%	0.0001%	0.0001%
B3	Number of users	10,000	10,000	10,000
Calc:	(B1*B2)*B3	$16,000	$16,000	$16,000

Source: Giga Information Group

Table 33: Exposure With Token Authentication

		Year 1	Year 2	Year 3
C1	Cost of unauthorized intrusion	$2,400,000	$2,400,000	$2,400,000
C2	Number of users	$10,000	$10,000	$10,000
C3	Possibility of fraud	0.0001%	0.0001%	0.0001%
Calc:	(C1*C2)*C3	$16,000	$16,000	$16,000

Source: Giga Information Group

Determining Costs

As in the case of the other two scenarios, costs were modeled for both the Entrust TruePass solution as well as the token authentication. In this scenario, we took into account the fact that this is a high-availability environment requiring redundant systems to protect the information from being corrupted.

In addition, we have incorporated into the Entrust TruePass solution the use of smart cards to provide a higher degree of security. As a result, the costs per user for the Entrust TruePass solution will be significantly increased due to the acquisition of smart cards and associated readers.

Table 34: Costs — Entrust TruePass

	Year 1	Year 2	Year 3
Software	$(639,176)	$(95,976)	$(95,976)
Hardware	$(419,600)	–	–
Internal IT costs	$(270,835)	$(75,000)	$(75,000)
End-user costs	$(120,833)	$(37,500)	$(37,500)
Total costs	$(1,450,445)	$(208,476)	$(208,476)

Source: Giga Information Group

Table 35: Costs — Token-Based Authentication

	Year 1	Year 2	Year 3
Software	$(474,000)	$(94,800)	$(94,800)
Hardware	$(679,200)	–	–
Internal IT costs	$(393,640)	$(76,000)	$(76,000)
End-user costs	$(120,833)	$(37,500)	$(37,500)
Total costs	$(1,667,673)	$(208,300)	$(208,300)

Source: Giga Information Group

Determining Risks

Risk was modeled using the same magnitude as in the other scenarios. Similar impacts were applied to the cost and benefit estimates contained within the model.

Flexibility

This scenario gave us a chance to model the potential flexibility of the Entrust solution as it applies to end-to-end encryption. Entrust digitally signs and encrypts transaction data at the browser and moves the encrypted data all the way to a back-end server for later decryption and signature verification. This avoids data exposure on the Web server where hackers can break in. As a result, the likelihood is reduced that a possible threat will not be discovered leading to a loss of potentially sensitive data.

As with all flexibility options, for this benefit to be achieved, it requires an additional investment above and beyond the investment for the initial Entrust TruePass solution. The cost in this case was the expense related to the additional licenses as well as the cost of integrating the end-to-end solution.

Table 36 reflects the assumptions used to construct the option value as well as the cost and benefit estimates used in the Black-Scholes Option Pricing Model. In this case, we are assuming that without persistent encryption in place, there is the potential for additional exposure related to patients records.

Table 36: Option Value of Persistent Encryption

Variable	Description	Amount	Value
S	Value of the assets associated with the future adoption of new business tools and methods	$448,347	Dollars
X	Spending required to acquire the assets	$150,000	Dollars
T	Length of time spending can be deferred (expiration)	2	Year(s)
R	Risk-free rate of return	6.50%	Years
σ	Market volatility, per year of potential assets — market-based	0.60	Per year
Black-Scholes Option Price (Value)		$323,070	

Source: Giga Information Group

Apart from persistent encryption, there are other things we did not model in terms of flexibility. These included the multi-use capability with smart cards, which could potentially add value but was not considered an option to the customers interviewed. In addition, the ability to use smart cards for multiple purposes such as storage of other security credentials, physical card access to the building and ID badge are functions that increase the value of flexibility of the Entrust TruePass solution.

Findings and Recommendations

As stated in the Executive Summary, the primary objective of this report is to illustrate the potential gains resulting from the deployment of a strong authentication solution. Organizations must apply the model contained within this report to their own circumstances to determine the impact of the given technology.

Table 37 illustrates the potential returns of using stronger authentication as compared to the use of passwords only, based on interviews of organizations using either Entrust TruePass or token authentication. All three scenarios provide a positive return based on the assumptions provided within this report. In all cases, the determinant value is based in part on the potential exposure of protected assets as well as the cost to protect. If the cost to protect is high, for example, and the value of the potential exposure is low, then the return on investment will be relatively low.

Table 37: Entrust TruePass Returns for Strong Authentication

Entrust TruePass	Scenario A	Scenario B	Scenario C
ROI	124%	150%	421%
Risk-adjusted ROI	68%	106%	335%

Source: Giga Information Group

Table 38: Token-Based Authentication Returns for Strong Authentication

Tokens	Scenario A	Scenario B	Scenario C
ROI	45%	75%	380%
Risk-adjusted ROI	18%	41%	299%

Source: Giga Information Group

This is seen in scenario A. In this case, the potential loss resulting from unauthorized access is relatively low, meaning a more cost-effective authentication solution could provide a higher return. In scenario B, the potential loss has grown, making the case for stronger authentication much more compelling. For the final scenario, where true two-factor authentication has been used, the returns mirror the potential damage that could be done without strong authentication. All three cases illustrate that determining which method of authentication should be used depends primarily on estimating the cost of exposing information.

As stated, the purpose is of this study is not to draw across the board conclusions around the success of one technology over another, but rather to show how TEI can illustrate the potential gains of a given solution. That said, the study resulted in several findings:

- The returns resulting from security are dependent on the specific potential of exposure and the cost associated with the loss of effective security around sensitive information.
- Based on the assumptions provided for each scenario, Entrust's TruePass product delivered a positive return in each of the three environments.
- Token-based authentication delivered a positive return in each of the three scenarios. Cases where the return was lower than the Entrust TruePass product were a result of primarily higher hardware costs associated with the purchase of the physical token.
- The Entrust TruePass solution provided more options for balancing security against scalability and cost control by allowing different user groups to access the same technology at different levels of authentication.

Appendix A

Calculations around the probability of expected losses and the average exposure to the representative companies were based on a combination of interviews, internal Giga discussions and external research. A sampling of external research used is cited here.

US General Accounting Office, “Identity Fraud: Information on Prevalence and Cost Appear to be Growing,” GAO 02-363 (Washington, DC, March, 2002).

CALPIRG (Sacramento, CA) and Privacy Rights Clearinghouse (San Diego, CA), “Nowhere to Turn: Victims Speak Out on Identity Theft” (May 2000).

Computer Security Institute, “2002 CSI/FBI Computer Crime and Security Survey,” Vol. VIII, No .1 (Spring 2002)

Appendix B

Non risk adjusted cash flow for Entrust TruePass and token authentication for each scenario:

Cash Flow — TruePass Scenario A		Year 1		Year 2		Year 3
Costs						
Software	$	(739,860)	$	(112,860)	$	(112,860)
Hardware	$	(80,000)	$	-	$	-
User Registration	$	(416,667)	$	-	$	-
Application Integration	$	(155,972)	$	-	$	-
Registration Administration	$	(300,000)	$	-	$	-
Ongoing Administration	$	(125,000)	$	(125,000)	$	(125,000)
Support — Help Desk	$	(187,500)	$	(187,500)	$	(187,500)
Total Costs	$	(2,004,999)	$	(425,360)	$	(425,360)
Benefits						
Corporate Loss Avoided	$	2,000,000	$	2,000,000	$	2,000,000
End-User Loss Avoided	$	66,667	$	66,667	$	66,667
Brand Costs Avoided	$	300,000				
Digital Signatures	$	182,408				
Total Benefits	$	2,549,075	$	2,066,667	$	2,066,667
Cash Flow	$	544,076	$	1,641,307	$	1,641,307
Net Present Value		$3,084,204.22				
ROI		124%				

Cash Flow — Token Authentication Scenario A		Year 1		Year 2		Year 3
Costs						
Software	$	(940,416)	$	(94,800)	$	(94,800)
Hardware	$	(1,637,600)	$	-	$	-
User Registration	$	(416,667)	$	-	$	-
Application Integration	$	(523,603)	$	-	$	-
Registration Administration	$	(300,000)	$	-	$	-
Ongoing Administration	$	(375,000)	$	(375,000)	$	(375,000)
Shipping	$	(100,000)	$	(5,000)	$	(5,000)
Support — Help Desk	$	(187,500)	$	(187,500)	$	(187,500)
Total Costs	$	(4,480,786)	$	(662,300)	$	(662,300)
Benefits						
Corporate Loss Avoided	$	2,625,000	$	2,625,000	$	2,625,000
End-User Loss Avoided	$	87,500	$	87,500	$	87,500
Brand Costs Avoided	$	300,000				
Total Benefits	$	3,012,500	$	2,712,500	$	2,712,500
Cash Flow	$	(1,468,286)	$	2,050,200	$	2,050,200
Net Present Value		$2,632,114.13				
ROI		45%				

Cash Flow — TruePass Scenario B		Year 1		Year 2		Year 3
Costs						
Software	$	(319,588)	$	(47,988)	$	(47,988)
Hardware	$	(80,000)	$	-	$	-
User Registration	$	(83,333)	$	-	$	-
Application Integration	$	(71,918)	$	-	$	-
Registration Administration	$	(60,000)	$	-	$	-
Ongoing Administration	$	(25,000)	$	(25,000)	$	(25,000)
Support — Help Desk	$	(37,500)	$	(37,500)	$	(37,500)
Total Costs	$	(677,339)	$	(110,488)	$	(110,488)
Benefits						
Corporate Loss Avoided	$	729,167	$	729,167	$	729,167
End-User Loss Avoided	$	35,000	$	35,000	$	35,000
Digital Signatures	$	82,320				
Total Benefits	$	846,487	$	764,167	$	764,167
Cash Flow	$	169,148	$	653,679	$	653,679
Net Present Value		$1,185,119.56				
ROI		150%				

Cash Flow — Token Authentication Scenario B	Year 1	Year 2	Year 3
Costs			
Software	$ (237,000)	$ (47,400)	$ (47,400)
Hardware	$ (599,200)	$ -	$ -
User Registration	$ (83,333)	$ -	$ -
Application Integration	$ (523,603)	$ -	$ -
Registration Administration	$ (60,000)	$ -	$ -
Ongoing Administration	$ (75,000)	$ (75,000)	$ (75,000)
Shipping	$ (20,000)	$ (1,000)	$ (1,000)
Support — Help Desk	$ (37,500)	$ (37,500)	$ (37,500)
Total Costs	$ (1,635,637)	$ (160,900)	$ (160,900)
Benefits			
Corporate Loss Avoided	$ 1,093,750	$ 1,093,750	$ 1,093,750
End-User Loss Avoided	$ 49,286	$ 49,286	$ 49,286
Total Benefits	$ 1,143,036	$ 1,143,036	$ 1,143,036
Cash Flow	$ (492,601)	$ 982,136	$ 982,136
Net Present Value	$1,471,670.61		
ROI	75%		

Cash Flow — TruePass Scenario C	Year 1	Year 2	Year 3
Costs			
Software	$ (639,176)	$ (95,976)	$ (95,976)
Hardware	$ (419,600)	$ -	$ -
User Registration	$ (83,333)	$ -	$ -
Application Integration	$ (135,835)	$ -	$ -
Registration Administration	$ (60,000)	$ -	$ -
Ongoing Administration	$ (75,000)	$ (75,000)	$ (75,000)
Support — Help Desk	$ (37,500)	$ (37,500)	$ (37,500)
Total Costs	$ (1,450,445)	$ (208,476)	$ (208,476)
Benefits			
Corporate Loss Avoided	$ 950,000	$ 950,000	$ 950,000
End User loss Avoided	$ 2,384,000	$ 2,384,000	$ 2,384,000
Digital Encryption	$ 323,070		
Total Benefits	$ 3,657,070	$ 3,334,000	$ 3,334,000
Cash Flow	$ 2,206,625	$ 3,125,524	$ 3,125,524
Net Present Value	$6,937,353.30		
ROI	421%		

Cash Flow -Token Authentication Scenario C		Year 1		Year 2		Year 3
Costs						
Software	$	(474,000)	$	(94,800)	$	(94,800)
Hardware	$	(679,200)	$	-	$	-
User Registration	$	(83,333)	$	-	$	-
Application Integration	$	(238,640)	$	-	$	-
Registration Administration	$	(60,000)	$	-	$	-
Ongoing Administration	$	(75,000)	$	(75,000)	$	(75,000)
Shipping	$	(20,000)	$	(1,000)	$	(1,000)
Support - Help Desk	$	(37,500)	$	(37,500)	$	(37,500)
Total Costs	$	(1,667,673)	$	(208,300)	$	(208,300)
Benefits						
Corporate Loss Avoided	$	950,000	$	950,000	$	950,000
End User loss Avoided	$	2,384,000	$	2,384,000	$	2,384,000
Total Benefits	$	3,334,000	$	3,334,000	$	3,334,000
Cash Flow	$	1,666,327	$	3,125,700	$	3,125,700
Net Present Value		$7,917,726.67				
ROI		380%				