A Forrester Total Economic Impact™ Study

Commissioned By

IBM Trusteer

Project Director:
Adrienne Capaldo

September 2016

The Total Economic Impact™ Of IBM Trusteer Solutions

A Single Company Analysis Of The Business Benefits And Cost Savings Enabled By IBM Trusteer Solutions

FORRESTER®

Table Of Contents

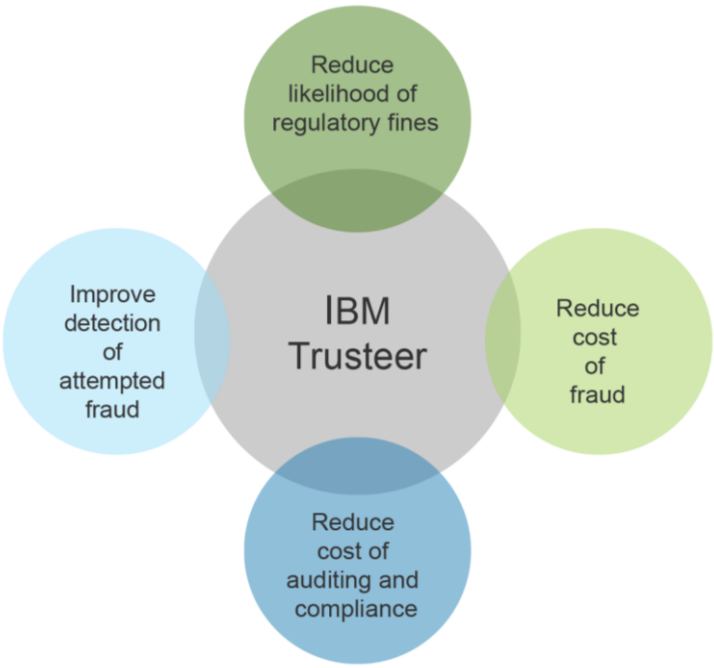
ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Executive Summary

Banking fraud is a widespread risk that has major consequences for financial institutions and their customer base. Fraud loss, fraud management costs, the costs associated with meeting regulatory and compliance needs, and brand reputation are just a handful of the factors that weigh on the minds of security and fraud teams. With innovative fraudsters and the ever-evolving nature of online fraud, financial service institutions must find cost-effective management fraud solutions that not only help mitigate today's risks but also prepare the organization for future scenarios.



Source: Forrester Research, Inc.

IBM commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying IBM Trusteer solutions. The purpose of this study is to provide readers with a framework to evaluate the potential financial benefit of IBM Trusteer Rapport and IBM Trusteer Pinpoint Detect to their organizations. IBM's Trusteer solutions support organizations to help identify and prevent fraud. IBM Rapport helps organizations protect against malware and phishing attacks through endpoint fraud protection, while IBM Trusteer Pinpoint Detect helps protect online banking sites against account takeover and fraudulent transactions and detects end user machines infected with high-risk malware in real time.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed an existing financial services organization with multiple years of experience using these Trusteer solutions.

IBM TRUSTEER SOLUTIONS REDUCED THE RISKS AND COSTS ASSOCIATED WITH FINANCIAL FRAUD

Our interview with an existing customer and subsequent financial analysis found that the interviewed organization experienced the risk-adjusted ROI and benefits shown in Figure 1. The analysis points to benefits of $8.7 million over three years versus total costs of $2.9 million, adding up to a net present value (NPV) of over $5.8 million.

FIGURE 1
Financial Summary Showing Three-Year Risk-Adjusted Results

ROI: 204%	NPV: $5,856,797	Payback: 8.5 months	90% reduction in the cost of fraud

Source: Forrester Research, Inc.

› **Benefits.** The interviewed organization experienced the following risk-adjusted benefits:

- **Ninety percent reduction in cost of fraud.** With both Rapport and Pinpoint Detect deployed, the organization is now able to prevent, quickly detect, and remediate malicious attacks, which significantly reduces its costs of fraud. As we heard from the organization, "In 2015, our fraud costs were approximately $7.5 million. This year, we have only had $750,000."
- **Eighty percent reduction in incidents of phishing and malware attacks.** The organization sees a reduction of 80% in the number of phishing and malware attacks it must address with the implementation of its Trusteer solutions.
- **Potential annual savings of $540,000 in regulatory fines.** Through its implementation of the IBM Trusteer solutions Rapport and Pinpoint Detect, the interviewed organization achieved compliance with its regulatory requirements, significantly reducing its risk of facing regulatory fines.
- **Fifty percent reduction in time spent on auditing and compliance preparations.** With easier access to required information, the Trusteer solutions helped cut down the time it takes the interviewed organization to prepare for an audit by half.

› **Costs.** The organization experienced the following risk-adjusted costs:

- **Cloud licensing and deployment/implementation services.** These are fees paid to IBM for the IBM Trusteer solutions, as well as professional services fees included for deployment and implementation services.
- **Internal implementation labor, ongoing support, and training.** These are the internal costs associated with the initial planning, implementation, and deployment of the Trusteer solutions, as well as those costs associated with the ongoing support, training, and change management of the Trusteer solutions.

Disclosures

The reader should be aware of the following:

› The study is commissioned by IBM and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

› Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the report to determine the appropriateness of an investment in the IBM Trusteer solutions.

› IBM reviewed 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.

› IBM provided the customer name for the interview but did not participate in the interview.

TEI Framework And Methodology

INTRODUCTION

From the information provided in the interview, Forrester has constructed a Total Economic Impact (TEI) framework for those organizations considering implementing IBM Trusteer. The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision.

APPROACH AND METHODOLOGY

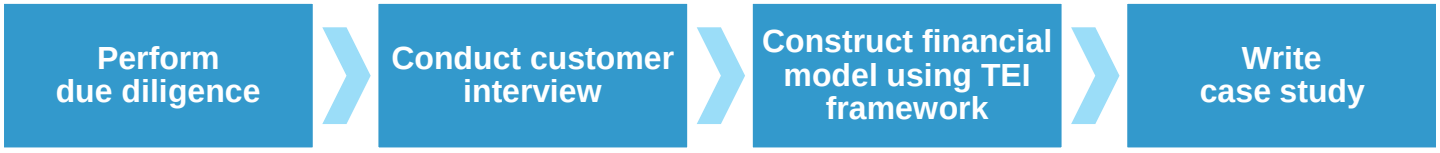
Forrester took a multistep approach to evaluate the impact that Trusteer can have on an organization (see Figure 2). Specifically, we:

- Interviewed IBM marketing, sales, and consulting personnel, along with Forrester analysts, to gather data relative to IBM Trusteer and the marketplace for IBM Trusteer solutions.
- Interviewed an organization currently using IBM Trusteer solutions to obtain data with respect to costs, benefits, and risks.
- Constructed a financial model representative of the interview using the TEI methodology. The financial model is populated with the cost and benefit data obtained from the interview.
- Risk-adjusted the financial model based on issues and concerns the interviewed organization highlighted in the interview. Risk adjustment is a key part of the TEI methodology. While the interviewed organization provided cost and benefit estimates, some categories could have a broad range of responses or had a number of outside forces that might have affected the results. For that reason, some cost and benefit totals have been risk-adjusted and are detailed in each relevant section.

Forrester employed four fundamental elements of TEI in modeling IBM Trusteer's impact: benefits, costs, flexibility, and risks.

Given the increasing sophistication that enterprises have regarding ROI analyses related to IT investments, Forrester's TEI methodology serves to provide a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

FIGURE 2
TEI Approach



Source: Forrester Research, Inc.

Analysis

INTERVIEWED ORGANIZATION

For this study, Forrester conducted an interview with the leader in the security and fraud department of a large financial services organization, an IBM Trusteer customer based in South America. The organization is a subsidiary of a global financial services organization. The global organization has many millions of customers and about 130,000 employees. The subsidiary Forrester interviewed has more than 12 million clients and 5,000 employees locally. Its customer base is made up of both retail and business users, and about 1.2 million of them use online banking. Based on this interview, Forrester constructed a TEI framework and an associated ROI analysis that illustrates the areas financially affected. The interview revealed that:

"[Criminals] will attack wherever they can — and obviously, they attack first where there is the most obvious problem, which is online banking for retail. That's where we had the highest quantity of affected clients."

~ Leader in security and fraud department

› Prior to implementing IBM Trusteer, the organization was using other third-party vendor software to support fraud prevention that was managed in-house. However, it found that these solutions alone were unable to meet all of its needs. The organization sought a solution that would enable it to add additional layers of security to help stop fraudulent activities. As we heard from the organization, "We made the decision that we needed a better tool." For one, its previous tools did not allow it to quickly adapt to new threats. In addition, the organization was only able to detect fraud after it happened — it lacked the ability to remediate those issues. "Before Trusteer, we only saw fraud passing by; we had no tools to prevent it. Many frauds were passing through [our old solution], but it was really just watching things happen without the tools to be able to stop it." In its previous environment, the organization lacked the tools to immediately block potential fraud. Finally, the software was managed in-house, which was time-consuming to the team.

› The interviewed organization initially implemented IBM Trusteer Rapport, and two years later deployed IBM Trusteer Pinpoint Detect. It currently has licenses to support 350,000 retail customers and 60,000 business customers for each solution. The organization plans to deploy IBM Trusteer Mobile SDK next year.

› Trusteer Rapport is endpoint fraud protection, downloaded directly onto the client device by the customer. It provides a layer of protection against phishing and man-in-the-browser (MITB) malware attacks. Using a network of tens of millions of endpoints across the globe, Trusteer Rapport collects intelligence on active phishing and malware attacks against organizations worldwide. Trusteer Rapport applies behavioral algorithms aimed to help block phishing attacks and prevent the installation and operation of MITB malware strains.

› Trusteer Pinpoint Detect is a clientless fraud protection software-as-a-service (SaaS) solution that works on the side of the online banking site, working in real time to detect, analyze, and help ensure that customer sessions are not fraudulent. Pinpoint Detect uses a series of indicators, such as device ID, behavior-based analytics, and behavioral anomalies to assess the risk of fraud in real time. It provides alerts in real time to remediate potential risk of fraud.

› Trusteer Mobile SDK works to help protect an organization's native mobile banking applications to proactively detect and help prevent fraud. The Trusteer Mobile SDK is designed to add another layer of protection to help provide safer mobile access to clients' applications, risk assessment of devices, pharming protection, and alert if device is using secure Wi-Fi.

Based on the interview, Forrester constructed a TEI framework and an associated ROI analysis that illustrates the areas financially affected.

INTERVIEW HIGHLIGHTS

Situation

Our interview uncovered the following drivers behind the organization's need for a new approach to fraud prevention:

› **The organization needed to meet regulatory and compliance requirements.** Financial services organizations operate in a highly regulated market, and they must comply with a wide variety of specifications. The onus is on the organizations to implement solutions that meet these fraud prevention requirements. Our interviewed organization is overseen by two regulatory bodies that require the organization meets a certain set of standards in fraud prevention. For fraud prevention and risk management, the organization told us: "[We] must have sufficient controls in order to prevent unrecognized, fraudulent transactions. We must have controls or tools that enable the identification of the customer, identify whether the client is the actual client, or if the client is at risk [for fraud]." The interviewed organization wanted to be proactive in ensuring it was meeting these standards. The organization also noted that it was obligated to offer free software to help prevent fraud.

> *"Before Trusteer, we only saw fraud passing by; we had no tools to prevent it."*
>
> ~ Leader in security and fraud department

› **The organization wanted to ensure it was protecting its customers and itself.** The organization had two main goals outside of compliance: It needed to protect itself, but it also needed to protect its customers. Internally, the organization needed to have the ability to protect against malware and phishing attacks and manage the risk associated with these activities. It needed a solution to prevent fraud losses, as well as keep the costs in check in regards to remediation. With its clients, the organization was focused on creating an environment where its customers felt safe and secure banking online. The organization understood the far-reaching impact that the security of its online sites had on its brand reputation and customer relationships. By taking a proactive approach to fraud prevention, the financial services institution hoped to both protect its customers from the negative impacts of fraud and further nurture high-quality, loyal relationships with its customer base. Combined, these two factors play a key role in ensuring this financial institution is protecting its brand.

› **The organization sought an approach to fraud prevention that was reliable, actionable, and helped reduce operational costs of fraud prevention.** The interviewed organization sought a technology solution that not only supported its fraud prevention goals but also created an efficient and effective environment for its security and fraud team. It required a reliable, accurate solution that would help to greatly reduce the number of false positive alerts it received and focus the team on actual fraudulent activities. It also needed a solution that enabled it to stop fraud on the spot. By finding a solution that successfully supported these needs, the organization could run a smarter security program that helped to reduce the operational costs of fraud prevention.

Solution

Integrating the Trusteer solutions with its existing fraud prevention processes and solutions, the organization was able to make a strong impact on its bottom line. Our interview uncovered that the financial services organization selected IBM's Security Trusteer solutions not only because they helped the organization with the above goals, but because they offer:

- **A holistic approach to fraud protection.** An important point that was brought up in our interviews was that, individually, these solutions offered high levels of protection against a variety of types of potential banking fraud. But our organization found that by employing multiple Trusteer solutions, it was able to build advanced layers of security that work in tandem to offer the highest levels of security to its own institution as well as its customers.
- **Trustworthy, sustainable, and adaptive fraud prevention against actual and potential new threats with actionable alerts.** IBM's Security Trusteer solutions work to continuously collect threat intelligence regarding active phishing and malware attacks from hundreds of millions of endpoints worldwide. Trusteer leverages that knowledge to create new algorithms to help stop actual and potential new threats. As new threats emerge, the financial services organization feels more confident in its protection and security with the use of IBM's risk analysis engine and learning. As we heard from the organization, "With this tool now, we no longer just see the fraud pass by; we are able to do something about it." These factors meant that the organization had a high degree of trust in the data coming out of the Trusteer solutions: "We have a major degree of certainty with the fraud it is detecting." The organization lacked this confidence with its previous solutions.
- **Scalable, easy-to-implement SaaS deployment.** IBM's Trusteer solutions were easy to use and implement. They brought the data the organization required for fraud prevention into one place, making it easy for the team to detect, remediate, and prevent malicious activity. Previously, the organization was responsible internally for updating and maintaining its fraud solutions, which added to its costs of operation.
- **Reputation protection.** When considering how best to protect its reputation, our interviewed organization looked for a solution that was well-trusted in the market. "Trusteer has definitely enabled us to avoid getting a reputation for fraud, and that . . . is so valuable, it's unquantifiable. And because we have millions of clients, the value of that reputation is very big." Working with IBM's team meant it was working with a best-in-class organization that helped support its goals.

BENEFITS

The interviewed organization experienced a number of quantified benefits in this case study:

- Reduction in cost of fraud.
- Reduced incidents of phishing and malware attacks.
- Reduction in likelihood of regulatory fines.
- Reduced time spent on auditing and compliance.

Reduction In Cost Of Fraud

Our first benefit looks at the reduction in the cost of fraud our organization has seen with its implementation of IBM Trusteer solutions. As we discussed, in its previous environment, the interviewed organization could only detect that fraud was happening, but it could not prevent and respond to or remediate the issue. With its deployment of Trusteer, the organization is now able to detect, prevent, and remediate issues with a high degree of accuracy. With both Rapport and Pinpoint Detect installed, the interviewed organization has seen a 90% reduction in the cost of fraud. "In 2015, our fraud costs were approximately $7.5 million. This year, we have only had $750,000."

To calculate the reduction in the cost of fraud, using the information gathered from the interview, we estimate the cost of fraud prior to the implementation of any of the Trusteer solutions to be $7.5 million. In Year 1, with the implementation of Rapport, the organization saw an estimated 15% reduction in the cost of fraud. By Year 2, as the fraud team became increasingly proficient in using Trusteer, this reduction increased to 25%. With the introduction of Pinpoint Detect, the organization saw a large jump to a 90% reduction in the cost of fraud. Before we continue, let's take a closer look at these numbers.

Looking at the percentage reduction in the cost of fraud numbers associated with Rapport and Pinpoint Detect, there are a few important factors to consider. Currently, the organization has made participation in Trusteer Rapport optional to its customer base. At the time Forrester spoke with the organization, its Rapport adoption was relatively low. As the organization told us, "We didn't do an aggressive campaign with clients to get them to download [Rapport], so we are perhaps not able to get the most benefits from it." The organization understands that to increase adoption, additional time and effort will be required to educate users on the benefits of downloading Rapport. As this is a solution that the customer must download, financial institutions that build a marketing plan around communicating the value of Rapport to their customer base see higher levels of adoption and higher levels of benefit.

When considering the potential impact of Rapport on the cost of fraud within your own organization, Forrester urges readers to consider several important factors:

- **Optional versus mandatory use.** In the case of the interviewed organization, it made the decision to keep Rapport as an optional download. Other organizations, based on their needs, may choose to make Rapport mandatory for their customers. Consider and weigh out the value of these methods when determining your approach to Rapport.
- **Time and effort in communicating the value.** Many organizations take a multichannel approach to marketing Rapport and promote adoption — educating their internal teams, creating online splash pages, and being in direct contact with clients are just some of the ways organizations work to communicate the value of downloading Rapport.

The higher the level of adoption, the larger the potential benefits your organization may receive from your investment in Rapport. When considering the value your organization could receive from an investment in Rapport, it is important to factor this into your analysis.

By introducing Pinpoint Detect into its environment, the interviewed organization immediately gained benefit from the extra layer of fraud prevention while minimizing the burden on the customer. It was impressed with how using these solutions in tandem dramatically decreased the cost of preventing fraud. By Year 3, using both Rapport and Pinpoint Detect, our interviewed organization decreased its fraud costs by 90% as compared with Year 1..

As we discussed, there are a number of variables that could potentially affect this calculation, particularly adoption. To assume for that risk, we have adjusted the benefit down by 15%, for a total three-year risk-adjusted benefit of $8,287,500. Table 1 shows how this benefit was calculated.

TABLE 1
Reduction In Cost Of Fraud

Ref.	Metric	Calculation	Rapport Year 1	Rapport Year 2	Rapport + PPD Year 3
A1	Cost of fraud prior to implementation of Trusteer solution		$7,500,000	$7,500,000	$7,500,000
A2	Percent reduction in cost of fraud with Trusteer solutions		15%	25%	90%
At	Reduction in cost of fraud	A1*A2	$1,125,000	$1,875,000	$6,750,000
	Risk adjustment	↓15%			
Atr	**Reduction in cost of fraud (risk-adjusted)**		**$956,250**	**$1,593,750**	**$5,737,500**

Source: Forrester Research, Inc.

Reduced Incidents Of Phishing And Malware Attacks

Our next benefit looks at how IBM Trusteer affected the number of phishing and malware attacks our interviewed organization saw, and how that affected the cost associated with managing those incidents. With the implementation of its Trusteer solutions, the organization improved its detection of potential fraud. It also saw a significant reduction in its number of phishing and malware attacks. It cited 100 incidents per week before Trusteer, and this decreased to 20 per week with both Rapport and Pinpoint Detect installed.

As we discussed earlier, the organization's previous environment did not allow it to prevent fraud. Now, it is able to quickly detect, block, and take action to remediate these attacks. The organization also cited that, with Trusteer, it had increased certainty around fraud — in its previous environment, it would receive false positives; with Trusteer, it felt more confident that these incidents were actual malicious attacks.

To calculate this benefit, Forrester assumes that prior to Trusteer, the organization saw 100 phishing and malware attacks per week, or 5,200 annually. With its investment in Rapport, it was able to reduce the number of attacks by 25%, to 3,900 attacks in Year 1. By Year 2, the organization reduced the number of attacks by 40%, with 3,120 attacks. By Year 3, with the introduction of Pinpoint Detect into its fraud prevention strategy, the organization saw an 80% reduction over Year 1 in the number of attacks its saw per week, reducing the number of annual attacks to 1,040. Forrester assumes that the fraud team spends 12 man-hours on each fraudulent attack. With fewer attacks, the fraud team is now able to focus on other value-add activities to further improve its overall fraud prevention strategy. However, it is unlikely that the time is used only on additional value-add

activities, so Forrester adjusted this benefit by assuming that only 50% of this time saved is used for productive work. Table 2 highlights how this was calculated.

As we saw previously, there are a number of factors that could affect the reduction in the number of malware and phishing attacks, as well as the time it takes to detect and respond to an attack. To compensate for these variations, Forrester has reduced the value of this benefit by 10%. Assuming an average fully loaded hourly salary of $36.06, the risk-adjusted total benefit over three years is $1,468,219.

TABLE 2
Reduced Incidents Of Phishing And Malware Attacks

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
B1	Number of phishing and malware attacks prior to investment in Trusteer	100 per week	5,200	5,200	5,200
B2	Number of phishing and malware attacks with Trusteer	(25%, 40%, 80% reduction)	3,900	3,120	1,040
B3	Time to detect and respond per attack	In hours	12	12	12
B4	Average hourly salary	F3	$36.06	$36.06	$36.06
B5	Percent productivity realized		50%	50%	50%
Bt	Reduced incidents of phishing and malware attack costs	(B1*B3*B4)-(B2*B3*B4) * B5	$281,268	$450,029	$900,058
	Risk adjustment	↓10%			
Btr	**Reduced incidents of phishing and malware attack costs (risk-adjusted)**		**$253,141**	**$405,026**	**$810,052**

Source: Forrester Research, Inc.

Reduction In Likelihood Of Regulatory Fines

Our third benefit looks at how, through the implementation of its IBM Trusteer solutions, the interviewed organization has reduced the likelihood of facing regulatory fines. Within the highly regulated financial services industry, there is significant risk associated with getting fined by a regulatory body for failure to comply with requirements. Through its investment in Trusteer, the organization is able to reduce the likelihood that it will be fined, as it is better able to meet the stringent rules and regulations it faces.

To calculate the potential risk, we look at the amount of the potential fine. The company estimates that the cost of the fine in any given year could be around $2 million without proper measures in place to prove compliance. This dollar amount will vary based on a number of factors and could significantly increase based on the type of fine. Forrester urges readers to consider the size of the potential fine they may face when calculating out the value of IBM Trusteer.

Forrester estimates that the probability of receiving a fine is about 30% in any given year. With the features and functionality of Trusteer, the organization is better able to meet its fraud prevention requirements and is now able to significantly reduce the likelihood of a regulatory fine. In Year 1, with the implementation of Rapport, we see a 75% reduction in the likelihood of a regulatory fine. As the fraud team becomes increasingly proficient in using

Trusteer, and with the additional layer of security brought in by Pinpoint Detect, the likelihood of a fine becomes less likely year after year. By Year 3, the organization sees a 90% reduced likelihood of a regulatory fine.

Forrester understands that there are a number of variables that could potentially affect this calculation. To assume for that risk, we have adjusted the benefit down by 15%, for a total three-year risk-adjusted benefit of $1,249,500.

TABLE 3
Reduction In Likelihood Of Regulatory Fines

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
C1	Average potential regulatory fine		$2,000,000	$2,000,000	$2,000,000
C2	Probability of a regulatory fine		30%	30%	30%
C3	Reduced likelihood of fine with Trusteer		75%	80%	90%
Ct	Reduction in likelihood of regulatory fines	C1*C2*C3	$450,000	$480,000	$540,000
	Risk adjustment	↓15%			
Ctr	**Reduction in likelihood of regulatory fines (risk-adjusted)**		**$382,500**	**$408,000**	**$459,000**

Source: Forrester Research, Inc.

Reduced Time Spent On Auditing And Compliance

Our final key benefit of the investment in Trusteer was the reduction in time spent on auditing and compliance needs. Through its implementation of Trusteer, the organization is now up to date with its regulatory compliance needs and has easier access to the information it needs to prove compliance in the event of an audit.

To calculate this benefit, the model assumes that prior to the implementation of Trusteer, the interviewed organization spent 160 man-hours gathering auditing and compliance information for each auditing event. We assume the organization sees an average of four auditing events each year, or one each quarter. Based on the experiences of our interviewed organization, we estimate that it is able to cut down the time spent on preparing for each audit event by 50%. With an average hourly compensation of $36.06, the interviewed organization saves nearly $11,500 each year in time spent on auditing and compliance.

Since time saved preparing for auditing and compliance needs will be dependent on the organization's prior processes and solutions, this benefit was risk-adjusted and reduced by 10%. The risk-adjusted total benefit resulting from the reduction in time spent on auditing and compliance needs over the three years was $31,156.

TABLE 4
Reduced Time Spent On Auditing And Compliance

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
D1	Man-hours spent gathering information for auditing and compliance needs per audit before Trusteer	4 weeks	160	160	160
D2	Number of audits per year	Conservatively estimate 1 per quarter	4	4	4
D3	Average hourly salary	F3	$36.06	$36.06	$36.06
D4	Percent reduction in time spent on auditing and compliance needs with Trusteer		50%	50%	50%
Dt	Reduced time spent on auditing and compliance	D1*D2*D3*D4	$11,539	$11,539	$11,539
	Risk adjustment	↓10%			
Dtr	**Reduced time spent on auditing and compliance (risk-adjusted)**		**$10,385**	**$10,385**	**$10,385**

Source: Forrester Research, Inc.

Total Benefits

Table 5 shows the total of all benefits across the four areas listed above, as well as present values (PVs) discounted at 10%. Over three years, the organization sees risk-adjusted total benefits to be a PV of more than $8.7 million.

TABLE 5
Total Benefits (Risk-Adjusted)

Ref.	Benefit Category	Year 1	Year 2	Year 3	Total	Present Value
Atr	Reduction in cost of fraud	$956,250	$1,593,750	$5,737,500	$8,287,500	$6,497,136
Btr	Reduced incidents of phishing and malware attacks	$253,141	$405,026	$810,052	$1,468,219	$1,173,464
Ctr	Reduction in likelihood of regulatory fines	$382,500	$408,000	$459,000	$1,249,500	$1,029,771
Dtr	Reduced time spent on auditing and compliance	$10,385	$10,385	$10,385	$31,156	$25,827
	Total benefits (risk-adjusted)	**$1,602,276**	**$2,417,161**	**$7,016,937**	**$11,036,375**	**$8,726,198**

Source: Forrester Research, Inc.

COSTS

The organization experienced a number of costs associated with the IBM Trusteer solutions:

- Costs for cloud licensing and deployment/implementation services.
- Internal implementation labor, ongoing support, and training.

These represent the mix of internal and external costs experienced by the organization for initial planning, implementation, and ongoing maintenance associated with the solution.

Costs For Licensing And Deployment/Implementation Services

These are fees paid to IBM for its IBM Trusteer solutions, as well as professional services fees included for deployment and implementation services. As a SaaS solution, the organization avoided costs associated with hardware needs, lowering its total cost of ownership. The interviewed organization signed a three-year contract with IBM for its Trusteer solutions, totaling a list price value of $3 million. To calculate this, our model assumes that the organization paid $1 million at contract signing for Year 1 (so the dollar value is accounted as an initial cost), and in subsequent years it paid at the beginning of each year (Year 2 is billed at the beginning of Year 2, and Year 3 is billed at the beginning of Year 3).

Trusteer costs can vary, depending on the number of licenses and number of solutions, as well as other factors. To compensate, this cost was risk-adjusted up by 5%. The risk-adjusted cost for IBM over the three years was $3.15 million. Table 6 below shows this calculation.

TABLE 6
Costs For Cloud Licensing And Deployment/Implementation Services

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
E1	Costs for cloud licensing and deployment/implementation services	Initial cost is for Year 1; Year 2 is billed at beginning of the year	$1,000,000		$1,000,000	$1,000,000
Et	Costs for cloud licensing and deployment/implementation services	E1	$1,000,000	$0	$1,000,000	$1,000,000
	Risk adjustment	↑5%				
Etr	**Costs for cloud licensing and deployment/implementation services (risk-adjusted)**		**$1,050,000**	**$0**	**$1,050,000**	**$1,050,000**

Source: Forrester Research, Inc.

Internal Implementation Labor, Ongoing Support, And Training

These are the internal costs associated with the initial planning, implementation, and deployment of the Trusteer solutions, as well as those costs associated with the ongoing support, training, and change management of the Trusteer solutions.

During the course of our interview, Forrester uncovered the importance this organization put on spending time upfront to fully plan out its Trusteer solutions implementation. The time deploying the actual SaaS solutions was not too laborious; however, to support a successful deployment, the interviewed organization made sure it put in the time upfront to fully plan out its implementation, in order to properly understand its end goals and the effects that deploying IBM Trusteer would have on the organization and customer base. As we heard from the organization: "Implementing Trusteer wasn't a very hard process. It's very short to actually implement. The biggest time is making sure you understand the project, that you understand the effects, that you do the testing."

During the first phase of implementation when the organization was deploying Rapport, it spent an estimated 350 man-hours for initial planning, testing, and deployment of Rapport. In subsequent years, the organization spends an estimated 400 man hours on ongoing support of the solutions. In Year 3, the organization spends an additional estimated 250 man-hours supporting the planning and deployment of its Pinpoint Detect solution. In addition, the organization incurs costs associated with training its employees and ongoing change management each year to ensure the success of its deployment. Table 7 below illustrates how this was calculated.

Resource costs, deployment time, and training and change management costs will vary from organization to organization. To compensate, this cost was risk-adjusted up by 5%. The total risk-adjusted cost of implementation and planning was $183,653.

TABLE 7
Internal Implementation Labor, Ongoing Support, And Training

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
F1	Man-hours for initial planning and implementation		350			250
F2	Annual number of man-hours for ongoing support			400	400	400
F3	Salary	$75,000/2,080 annual working hours	$36.06	$36.06	$36.06	$36.06
F4	Training and change management costs		$50,000	$20,000	$20,000	$20,000
Ft	Internal implementation labor, ongoing support, and training	((F1+F2)*F3)+F4	$62,621	$34,424	$34,424	$43,439
	Risk adjustment	↑5%				
Ftr	**Internal implementation labor, ongoing support, and training (risk-adjusted)**		**$65,752**	**$36,145**	**$36,145**	**$45,611**

Source: Forrester Research, Inc.

Total Costs

Table 8 shows the total of all costs as well as associated present values (PVs), discounted at 10%. Over three years, the organization expects risk-adjusted total costs to be a PV of about $2.9 million.

TABLE 8
Total Costs (Risk-Adjusted)

Ref.	Cost Category	Initial	Year 1	Year 2	Year 3	Total	Present Value
Etr	Costs for cloud licensing and deployment/implementation services	$1,050,000	$0	$1,050,000	$1,050,000	$3,150,000	$2,706,649
Ftr	Internal implementation labor, ongoing support, and training	$65,752	$36,145	$36,145	$45,611	$183,653	$162,752
	Total costs (risk-adjusted)	**$1,115,752**	**$36,145**	**$1,086,145**	**$1,095,611**	**$3,333,653**	**$2,869,401**

Source: Forrester Research, Inc.

FLEXIBILITY

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for some future additional investment. This provides an organization with the "right" or the ability to engage in future initiatives but not the obligation to do so. There are multiple scenarios in which a customer might choose to implement IBM Trusteer solutions and later realize additional uses and business opportunities. Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

Within the next year, the organization plans to launch Trusteer Mobile SDK to help protect its customers when using mobile apps. To provide an additional protection layer, IBM Trusteer mobile solutions can integrate with IBM Trusteer Pinpoint Detect using an embedded software development kit. This component assesses risk information from the mobile device — such as malware infections, root and jailbroken information, accurate geolocation, and Wi-Fi security status. As we heard from the interviewed company: "We are right now getting involved in mobile because we've seen an exponential increase in the number of customers who are using mobile for banking. Within the next year, mobile is going to be an important place to focus the team." the organization believes this will help them see additional benefits tied to further reduction of the costs associated with fraud, as well as help reduce the number of malicious attacks and the costs associated with them. This will also likely have an impact on its brand reputation and the trust that their customer base has in the interviewed organization.

In addition, with the inherent scalability of the SaaS Trusteer solutions, the organization can easily add more licenses as it continues to grow and needs to support a larger customer base.

RISKS

Forrester defines two types of risk associated with this analysis: "implementation risk" and "impact risk." Implementation risk is the risk that a proposed investment in Trusteer may deviate from the original or expected requirements, resulting in higher costs than anticipated. Impact risk refers to the risk that the business or technology needs of the organization may not be met by the investment in Trusteer, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for cost and benefit estimates.

TABLE 9
Benefit And Cost Risk Adjustments

Benefits	Adjustment
Reduction in likelihood of regulatory fines	↓ 15%
Reduction in cost of fraud	↓ 15%
Reduced incidents of phishing and malware attack costs	↓ 10%
Reduced time spent on auditing and compliance	↓ 10%

Costs	Adjustment
Costs for cloud licensing and deployment/implementation services	↑ 5%
Internal implementation labor, ongoing support, and training	↑ 5%

Source: Forrester Research, Inc.

Quantitatively capturing implementation risk and impact risk by directly adjusting the financial results provides more meaningful and accurate estimates and a more accurate projection of the ROI. In general, risks affect costs by raising the original estimates, and they affect benefits by reducing the original estimates. The risk-adjusted numbers should be taken as "realistic" expectations since they represent the expected values considering risk.

The following impact risks that affect benefits are identified as part of the analysis:

- Slower adoption than anticipated.
- Employees resisting using new processes and methodologies through the Trusteer solution.
- Variability in the value gained from the solution.

The following implementation risks that affect costs are identified as part of this analysis:

- Internal labor needed for planning and implementation higher than expected.
- Deployment takes longer than expected.
- Training requires more time than expected.

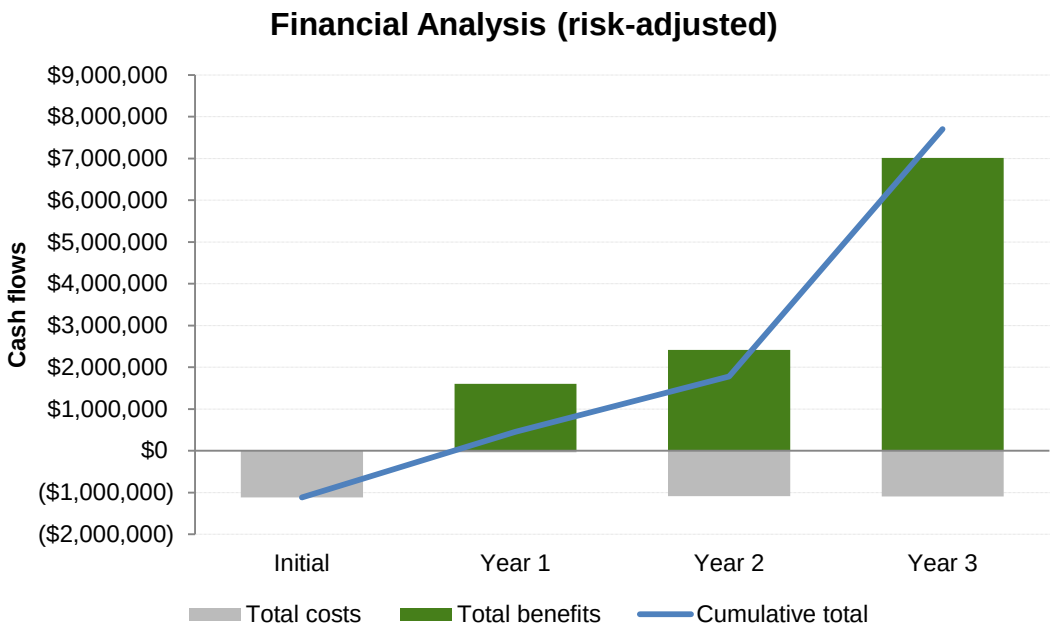
Table 9 shows the values used to adjust for risk and uncertainty in the cost and benefit estimates for the interviewed organization. Readers are urged to apply their own risk ranges based on their own degree of confidence in the cost and benefit estimates.

Financial Summary

The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the interviewed organization's investment in IBM Trusteer solutions.

Table 10 below shows the risk-adjusted ROI, NPV, and payback period values. These values are determined by applying the risk-adjustment values from Table 9 in the Risks section to the unadjusted results in each relevant cost and benefit section.

FIGURE 3
Cash Flow Chart (Risk-Adjusted)



Source: Forrester Research, Inc.

TABLE 10
Cash Flow (Risk-Adjusted)

Summary	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($1,115,752)	($36,145)	($1,086,145)	($1,095,611)	($3,333,653)	($2,869,401)
Total benefits	$0	$1,602,276	$2,417,161	$7,016,937	$11,036,375	$8,726,198
Total	**($1,115,752)**	**$1,566,131**	**$1,331,016**	**$5,921,326**	**$7,702,721**	**$5,856,797**
ROI						**204%**
Payback period (months)						**8.5**

Source: Forrester Research, Inc.

IBM Trusteer Solutions: Overview

The following information is provided by IBM. Forrester has not validated any claims and does not endorse IBM or its offerings.

The IBM® Trusteer® Fraud Protection Suite offers a simplified approach to fraud management to help your organization more accurately identify and prevent fraud — all while helping to lower costs and improve the end user experience.

IBM Trusteer Rapport helps protect malware and phishing attacks that are the root cause of most financial fraud. It also helps financial institutions to maximize protection of their customers, achieve sustainable fraud prevention, and meet regulatory compliance requirements.

IBM Trusteer Rapport provides:

- Multilayered protection to help protect user devices against malware infections and phishing attacks.
- Protection of web browser sessions to prevent tampering of customer transactions.
- Defense against identity fraud to help safeguard personal information.
- Protection against malware infections and removal of existing malware to create a safer online banking experience for customers.
- Protection against phishing of login credentials and payment card data to help preserve private information.

IBM Trusteer Pinpoint Detect helps protect its online banking sites against account takeover and fraudulent transactions and helps detect end user machines infected with high-risk malware. Financial institutions can detect fraud in real time through a full risk assessment based on a comprehensive user profile.

When users access their online banking site, IBM Trusteer Pinpoint Detect:

- Correlates device and session attributes to generate a complex device identifier.
- Analyzes user behavior.
- Detects potential device spoofing.
- Identifies access using compromised credentials.

To provide an additional protection layer, IBM Trusteer mobile solutions can integrate with IBM Trusteer Pinpoint Detect using an embedded software development kit. This component assesses risk information from the mobile device — such as malware infections, root and jailbroken information, accurate geolocation, and Wi-Fi security status.

IBM Trusteer Mobile SDK helps protect organizations' native mobile applications by performing device risk factors analysis and also provides a persistent mobile device ID. Trusteer Mobile SDK offers a library that enables application security services for mobile applications. This library can be used to build your custom application with Trusteer Mobile SDK's advanced security features. The core functionality provided by the library is as follows:

- Device hygiene.
- Persistent device identifiers
- Identity and risk analytics (including behavioral elements such as location and risk integration with IBM Trusteer Pinpoint Detect).

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. TEI assists technology vendors in winning, serving, and retaining customers.

The TEI methodology consists of four components to evaluate investment value: benefits, costs, flexibility, and risks.

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 form 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.

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. However, having the ability to capture that benefit has a PV that can be estimated. The flexibility component of TEI captures that value.

RISKS

Risks measure the uncertainty of benefit and cost estimates contained within the investment. Uncertainty is measured in two ways: 1) the likelihood that the cost and benefit estimates will meet the original projections and 2) the likelihood that the estimates will be measured and tracked over time. TEI risk factors are based on a probability density function known as "triangular distribution" to the values entered. At a minimum, three values are calculated to estimate the risk factor around each cost and benefit.

FRAMEWORK ASSUMPTIONS

Table 11 provides the model assumptions that Forrester used in this analysis.

The discount rate used in the PV and NPV calculations is 10%, and the time horizon used for the financial modeling is three years. Organizations typically use discount rates between 8% and 16% based on their current environment. Readers are urged to consult with their respective company's finance department to determine the most appropriate discount rate to use within their own organizations.

TABLE 11
Model Assumptions

Ref.	Metric	Calculation	Value
X1	Hours per week		40
X2	Weeks per year		52
X3	Hours per year (M-F, 9-5)		2,080
X4	Hours per year (24x7)		8,736
X5	Fully loaded compensation		$75,000
X6	End user average hourly compensation	(X5/X3)	$36.06

Source: Forrester Research, Inc.

Appendix B: Glossary

Discount rate: The interest rate used in cash flow analysis to take into account the time value of money. Companies set their own 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 respective organizations 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 NPV of cash flows.

Payback period: The breakeven point for an investment. This is 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 the Framework Assumptions section) at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations are not calculated until the summary tables are the sum of the initial investment and the discounted cash flows in each year.

Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

TABLE [EXAMPLE]
Example Table

Ref.	Metric	Calculation	Year 1	Year 2	Year 3

Source: Forrester Research, Inc.