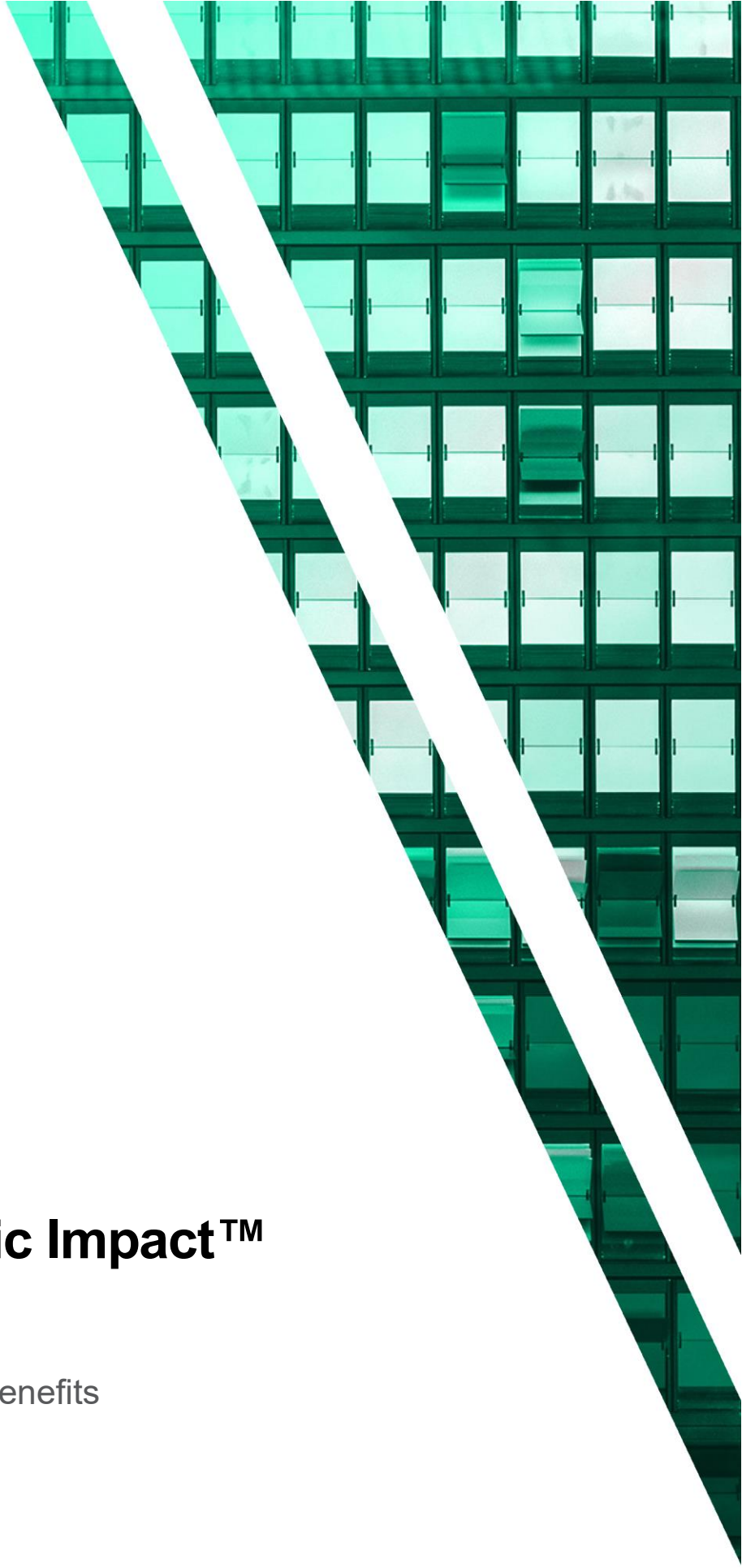
FORRESTER®



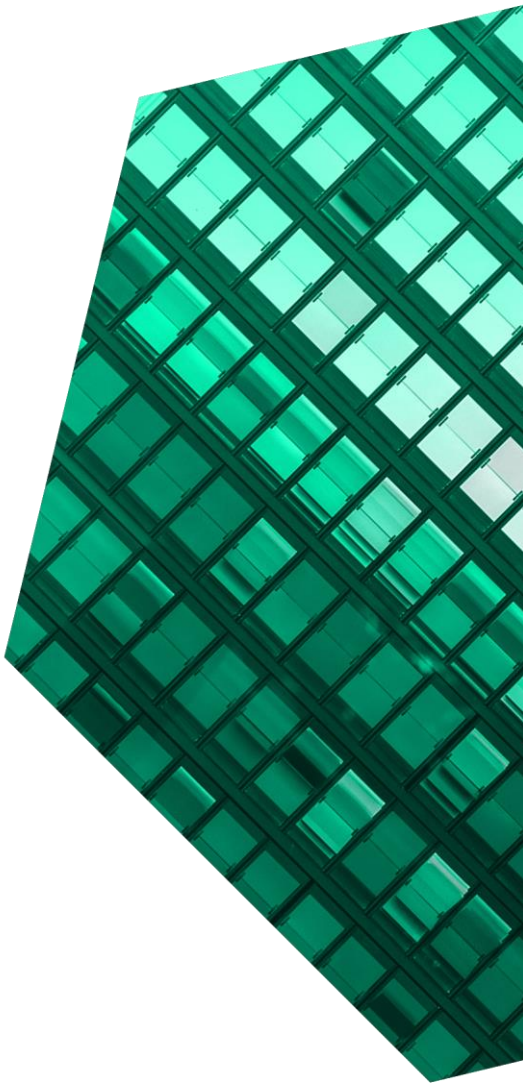
The Total Economic Impact™ Of Dataminr

Cost Savings And Business Benefits Enabled By Dataminr

JANUARY 2022

Table Of Contents

TEI Consultant: Eric Hall



Executive Summary

Due to an increasingly complex and challenging world, incidents are on the rise that put physical assets and employees at risk, disrupt business operations, reduce employee productivity, and affect the perceptions of customers and employees. Dataminr's artificial intelligence (AI)-based platform provides real-time alerts about high impact incidents from more than 250,000 public data sources worldwide. Critical alerts typically arrive more than 45 minutes before other solutions with context, images, videos, and links to sources.

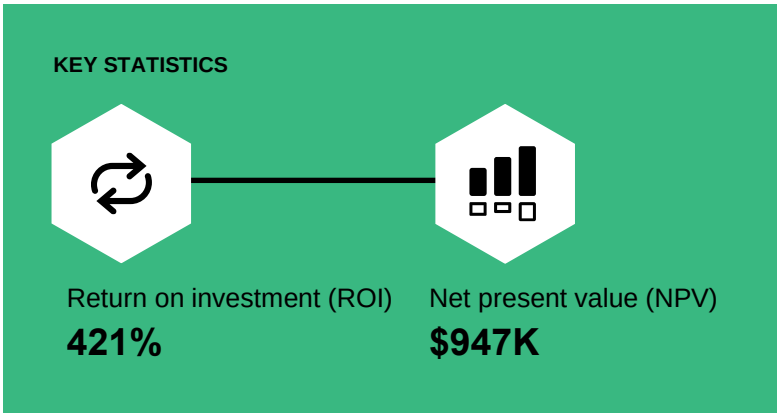
Dataminr utilizes real-time AI to provide event and risk detection within publicly available data. Dataminr uses a range of deep learning AI methods from a number of scientific fields, including natural language processing, understanding, and generation; computer vision; audio processing and classification; and anomaly detection on both machine- and human-generated public data streams. This study primarily focuses on the use of Dataminr for incident detection for security and risk mitigation to protect people and assets, to minimize business disruption, and to provide brand and reputational protection; however, additional use cases include cyber threat intelligence and business intelligence.

Dataminr commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Dataminr.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Dataminr on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five decision-makers with experience using Dataminr. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization.

Prior to using Dataminr, these interviewees noted how their corporate security organizations typically learned of incidents that affected them not soon enough to effectively react to the incidents, or after news organizations announced them. Interviewees also noted that their current tools and sources lacked 24/7 coverage, provided excessive false positives, often did not adequately cover certain global areas, and lacked sufficient translation capabilities. For organizations building out a corporate security function, interviewees expressed concern about the cost of traditional analyst-based alerting services.

After the investment in Dataminr, the interviewees noted that most actionable incidents were first identified by Dataminr — and sometimes only by Dataminr. Key results from the investment include informative alerts more than 45 minutes before other sources, the ability to personalize alert settings that deliver more relevant alerts, 24/7 coverage per Dataminr's real-time AI alerting, and both labor and tool/service cost savings.



KEY FINDINGS

Quantified benefits. Risk-adjusted present value (PV) quantified benefits over three years include:

- **Avoided facility closures and mobile/field employee disruptions, providing benefits worth more than $400,000.** Dataminr provides customers with early alerts that allow them to relocate mobile/field workers to avoid work loss. It also features early notifications to prepare for power outages or minimize physical asset disruptions by preventing closures, delaying closures, or hastening reopenings and to prepare for power outages and other disruptions.

"Speed to action and control of the narrative is absolutely critical in this information age where things can get sensationalized or people can get misinformed very quickly."

Crisis and risk manager, manufacturing

- **Avoided or reduced reputation damage due to crises or critical events, and associated recovery costs, providing benefits worth more than $201,000.** Customers have been able to avoid or reduce reputational damage from crises or critical events by being able to act sooner and communicate better. This may eliminate or reduce the magnitude of reputational damage and in doing so, also reduce the cost to recover from the damage.
- **Incident remediation cost savings by reducing duplicative or unnecessary effort, providing benefits worth almost $80,000 over three years.** By receiving alerts on incidents typically more than an hour before the news media covers them, Dataminr customers can develop an action plan and notify key internal leaders of the incident as well as the actions being taken, thus reducing duplicative actions by others or actions by others that would not be beneficial.
- **Avoided corporate security labor and reduced software costs, providing benefits worth more than $391,000.** Corporate security teams have been able to reduce labor costs by using Dataminr alerts to provide needed 24/7 coverage and with personalized alert settings and routing. so the right alerts go to the right people. Due to Dataminr's breadth of data sources, strong AI capabilities, and comprehensive alerting, corporate security teams are able to reduce use of other threat-alerting tools.
- **Avoided labor cost to provide necessary early warnings and coverage from data sources not available in other solutions, providing benefits worth more than $122,000.** Customers recognize that receiving an alert even 30 minutes sooner than from other tools may have significant repercussions on employee safety or brand reputation risk. Without Dataminr they would have to augment other tools with their own efforts to meet this need. Customers that have expanded into emerging markets recognize that Dataminr draws data from important sources that other tools do not, so they would need to augment those tools to get valuable alerts.

Unquantified benefits. Benefits that are not quantified for this study include:

- **Saving human life.** Most interviewees spoke of specific events where Dataminr alerts led to early action that they considered significant toward protecting employees, customers, or other workers.

- **Maintaining an employee-first reputation.** Interviewed decision-makers described how their corporate security team's actions to protect employees demonstrate a commitment to their well-being, which was recognized internally by employees.

"When we trialed Dataminr, we got information about two employee-related security events, 15 and 45 minutes earlier than our existing information channels. This ability to react much earlier to protect our employees made our decision for us."

Global head of security operations, enterprise software

- **Securing the trust of corporate leadership.** Interviewees noted that their relationship with corporate leadership improved because of their ability to act quickly and decisively using Dataminr.
- **Proactive action that keeps the company out of the limelight reduces future guilt by association.** Many benefits will increase over time by preventing the repeated association of the company or product with crises and critical events. There is no practical way to estimate that improvement financially.
- **Being supported by a strong customer success team.** Interviewees called out the Dataminr customer success and account management teams, support functions that are included in the base contract, as crucial partners in ensuring the success of the corporate security function. They work to understand goals and needs, personalize account settings, provide training, assess and improve performance, and share best practices.
- **Monitoring pandemic risks.** Some of the customers used Dataminr's COVID-19 tracking, where Dataminr associated spikes in social media posts in areas just prior to COVID-19 flare-ups. This proved useful at times in making early decisions, but in general it let customers know where to focus their attention.

Costs. Risk-adjusted PV costs over three years include setup, training, and licensing costs of $225,000 over three years**.** Dataminr only charges an annual licensing subscription fee. Setup and training costs are internal costs only.

The decision-maker interviews and financial analysis found that a composite organization experiences benefits of $1.17 million over three years versus costs of $225,000, adding up to a net present value (NPV) of $947,000 and an ROI of 421%.

"Folks love the way Dataminr has incident alerts packaged with sources, photos, and videos. They have told me that they want more Dataminr and less of the other alerting."

Head of intelligence, travel and hospitality

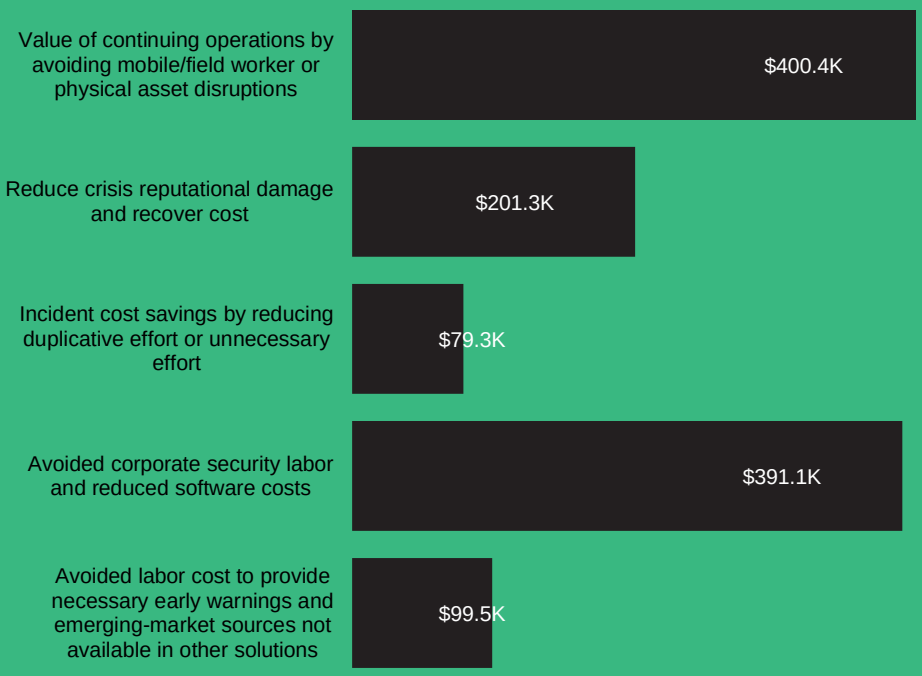
ROI
421%

BENEFITS PV
$1.17M

NPV
$947K

PAYBACK
<6 months

Benefits (Three-Year)



“Over 90% of our critical events are identified with Dataminr first. Dataminr is identifying crises and greater-impact incidents that affect the marketplace. We are protecting employees and brand with Dataminr.”

— Global security center manager, technology

TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in Dataminr.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that Dataminr can have on an organization.

DUE DILIGENCE

Interviewed Dataminr stakeholders and Forrester analysts to gather data relative to Dataminr.

DECISION-MAKER INTERVIEWS

Interviewed five decision-makers at organizations using Dataminr to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewees' organizations.

FINANCIAL MODEL FRAMEWORK

Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the decision-makers.

CASE STUDY

Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The Dataminr Customer Journey

Drivers leading to the Dataminr investment

Interviewed Decision-Makers

Interviewee	Industry	Notable Assets	Annual Revenue
Global head of security operations	Enterprise software	100,000+ employees 100+ physical assets	$20+ billion
Head of intelligence	Travel and hospitality	100,000+ employees 5,000+ physical assets	$4+ billion
Global security center manager	Technology	10,000+ field/mobile workers	$10+ billion
CSO	Data analytics and technology	10,000+ field/mobile workers	$2+ billion
Crisis and risk manager	Manufacturing	10,000+ physical assets	$20+ billion

KEY CHALLENGES

Two types of customers were interviewed for this TEI study: organizations ramping up their corporate security organization and organizations with a relatively mature corporate security function that recognized that it was unable to fulfill its corporate security and risk-mitigation responsibilities.

The interviewees noted how their organizations struggled with common challenges before working with Dataminr, including:

- **The need for earlier alerts.** It has become more and more common for events around the world to put employees at risk or cause major corporate or brand reputation damage. Interviewees noted that every minute counts when acting on these incidents.
- **Lack of 24/7 coverage.** Interviewees shared that analyst-based alerting services are typically not provided on a 24/7 basis, so delays in notifications can be hours after the incident starts.
- **Gaps in breadth of data.** Interviewees noted that there were frequently times when they did not learn about certain incidents, which impacted their ability to respond.

> **"Non-English-speaking markets are very important to us. Some of our tools' translations are so bad that we literally have no idea what they're talking about. We want to know about fires in Indonesia and stabbings in Uganda and riots in Nigeria, all that stuff. The other vendors are all pretty good at tracking stuff in the US and Western Europe, where the government is putting out good information, but it's very different in other countries."**
>
> *Head of intelligence, travel and hospitality*

- **Poor translations.** Language translations that served global operations were typically decent, but interviewees noted that they felt that they could have been more accurate and clearer.

- **Expensive analyst services.** Interviewees from less mature corporate security functions had a hard time justifying more expensive services that involve analysts creating reports about incidents.
- **Corporate security lacking internal trust.** Interviewees spoke of trust about their ability to effectively perform their role. A big part of this perception was because leadership and other employees frequently learned of major incidents through news outlets, not from corporate security.

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the five decision-makers that Forrester interviewed and is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The global, multibillion-dollar organization can have either a mature corporate security organization, with multiple associated tools, or an evolving corporate security function that is both adding tools and adding staff. The composite organization has moderate brand risk, meaning that involvement in crises or other critical events, either directly or indirectly, will cause corporate and brand reputation damage.

Deployment characteristics. The organization has 15,000 employees, 2,500 of whom are either mobile or field workers. There are five regions or business units, each with a corporate security team member. There are 2,500 physical assets monitored by Dataminr. The central corporate security team has five members, and the annual spend on security and risk management software is $500,000. There are two crises or critical events per year that may disrupt their business operations or cause global or regional reputation damage.

Key assumptions

- **Global organization**
- **$10 billion annual revenue**
- **Moderate brand reputation risk**
- **2,500 mobile/field workers**
- **2,500 physical assets**
- **Five regions or business units**
- **Five-member central security team**

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Value of continuing operations by avoiding mobile/field worker or physical asset disruptions	$161,000	$161,000	$161,000	$483,000	$400,383
Btr	Avoided or reduced reputational damage due to crises and associated recovery cost	$80,000	$81,000	$82,050	$243,050	$201,315
Ctr	Incident cost savings by reducing duplicative effort or unnecessary effort	$31,875	$31,875	$31,875	$95,625	$79,268
Dtr	Avoided corporate security labor and reduced software costs	$157,250	$157,250	$157,250	$471,750	$391,057
Etr	Avoided labor cost to provide necessary early warnings and emerging-market sources not available in other solutions	$40,000	$40,000	$40,000	$120,000	$99,474
	Total benefits (risk-adjusted)	$470,125	$471,125	$472,175	$1,413,425	$1,171,497

VALUE OF CONTINUING OPERATIONS BY AVOIDING MOBILE/FIELD WORKER OR PHYSICAL ASSET DISRUPTIONS

Evidence and data. Interviewees spoke of Dataminr providing early alerts that eliminated or reduced the cost of disruptions to mobile/field workers and physical assets, including:

- Labor savings by relocating mobile/field workers to avoid work loss. Benefits include a combination of labor productivity and reductions in revenue loss and service-level penalties.
- Facility downtime disruptions reduced due to early notifications of likely power outages, allowing time to get backup generators or timely notifications that may prevent or delay closures until necessary.

Modeling and assumptions. Based on customer interviews, Forrester estimates the following for the composite organization:

- The average risk of disruption per worker is 0.5 days per year.
- The average cost per mobile/field worker is $144 per day.
- Prior to Dataminr, 0.5% of physical assets had disruptions annually.
- Dataminr prevents 5% of physical asset disruptions.
- The average cost per disruption at a physical asset site is $250,000.

"If we did not have Dataminr, we would not be able to be as effective and make the kind of decisions we did with confidence. We'd be just guessing. We have over 90% of field personnel back at work; without Dataminr we would probably have 70% or less back at work."

CSO, data analytics and technology

Risks. Risks that could impact the realization of this benefit include:

- The number of mobile/field workers within an organization.
- The sensitivity workers have to work disruptions based upon incident types.
- The hourly cost of disruption per worker, which will vary based on labor cost, revenue loss, flexible hours, or other factors.
- The organization's physical asset count.
- The risk, historical frequency, and cost of disruption per asset, which will vary by location, type of asset, condition of asset, and other factors.

"When there is a risk of power outages, having a 30-minutes-earlier lead time on getting emergency generators to an office or data center can really make a difference towards keeping the power on."

Global head of security operations, enterprise software

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of more than $400,000.

Value Of Continuing Operations By Avoiding Mobile/Field Worker Or Physical Asset Disruptions

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Mobile and field workers	Composite	2,500	2,500	2,500
A2	Average annual days at risk of disruption per worker	Composite	0.5	0.5	0.5
A3	Cost per day per field worker	Composite	$144	$144	$144
A4	Percentage of disruptions averted by Dataminr early warnings	Interviews	25%	25%	25%
A5	Subtotal: cost reduction associated with reducing disruption of mobile and field workers	A1*A2*A3*A4	$45,000	$45,000	$45,000
A6	Physical asset count	Composite	2,500	2,500	2,500
A7	Percentage of assets with disruptions historically (annual)	Composite	0.5%	0.5%	0.5%
A8	Percentage of disruptions averted due to Dataminr alerts	Interviews	5.0%	5.0%	5.0%
A9	Cost per disruption at physical asset sites	Composite	$250,000	$250,000	$250,000
A10	Subtotal: cost reduction associated with reducing disruption at physical asset sites	A6*A7*A8*A9	$156,250	$156,250	$156,250
At	Value of continuing operations by avoiding mobile/field worker or physical asset disruptions	A5+A10	$201,250	$201,250	$201,250
	Risk adjustment	↓20%			
Atr	Value of continuing operations by avoiding mobile/field worker or physical asset disruptions (risk-adjusted)		$161,000	$161,000	$161,000
	Three-year total: $483,000			**Three-year present value: $400,383**	

AVOIDED OR REDUCED REPUTATION DAMAGE DUE TO CRISES AND ASSOCIATED RECOVERY COSTS

Evidence and data. Interviewees described varying degrees of reputation risk associated with crises and critical events, as well as the organization's ability to handle them.

- Organization and brand reputation were harmed due to incidents involving physical property, products, employees as victims, and employees as culprits.
- Both internal and external resources were involved in dealing with the repercussions of the crises and critical events, whether by handling the direct results of them, employee-related communications, reputation recovery activities, investigations, or other follow-up activities.

"There is tremendous value in our knowing events within our industry almost immediately. … The media reaches out immediately, and we can't come across as defensive or elusive; we need to know as much as possible. Leadership needs to prepare for shareholders — they want to know if we had a role in the event and what actions we are taking. … Our customers want to know that we are aware of the event, [are] troubleshooting, have a plan of action, and [are] not delaying anything in the process."

Crisis and risk manager, manufacturing

Modeling and assumptions. Based on customer interviews, Forrester estimates the following for the composite organization:

- The number of crises or critical events per year was not directly related to any specific attribute of the five organizations, but an association of revenue was made, supporting a likelihood of two crises or critical events per year.
- The average cost of recovery efforts, including legal, public relations, and marketing, is $300,000 per crisis.
- Dataminr provides alerts and insights that help prevent or reduce the magnitude of the crises or critical events by 25%.
- Revenue loss from the average crisis or critical event is assumed to be 0.01% for this $10 billion per year composite organization.
- The composite organization's profit margin is 10%.
- The reputation risk to the five interviewees' organizations varied significantly, which is associated with the resulting recovery effort and revenue loss. The composite organization has a medium-level reputation risk, so the recovery cost and revenue loss are reduced by 50%.

Risks. Risks that could impact the realization of this benefit include:

- The number of crises and critical events per year, average incident severity, and average recovery cost will vary significantly by industry, organization size, organization locations, visibility of organization leadership, and other factors.
- Dataminr's ability to identify potential or active crises/critical events will vary based on the availability and sharing of information, videos, and images within Dataminr's 250,000+ data sources.

"We call ourselves "People Protect," so the focus is on protecting our assets, and our most valuable asset is our employees. To do that effectively requires both speed and actionable alerts — both Dataminr strengths. When we protect our employees, we are protecting our brand, as a company and as an employer."

Global head of security operations, enterprise software

- The amount of revenue loss per crisis will vary significantly based upon the types of crises that occur, organization characteristics, product characteristics, and perceptions resulting from media coverage, among other factors.
- Profit margins vary by organization.
- The brand risk exposure will vary significantly for organizations, leading to dramatic differences in both reputation recovery costs and revenue loss.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of more than $201,000.

Avoided Or Reduced Crisis Reputational Damage Due To Crises And Associated Recovery Costs

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Crises per year	Composite	2	2	2
B2	Average cost per crisis for high-brand-exposure company (legal, marketing, PR, etc.)	Composite	$300,000	$300,000	$300,000
B3	Percentage of cost mitigation or elimination associated with recovery efforts	Interviews	25%	25%	25%
B4	Subtotal: recovery cost reduction	B1*B3*B2	$150,000	$150,000	$150,000
B5	Annual revenue	Composite	$10,000,000,000	$10,500,000,000	$11,025,000,000
B6	Percentage of revenue loss per crisis	Interviews	0.01%	0.01%	0.01%
B7	Average revenue loss per crisis	B5*B6*1,000,000	$1,000,000	$1,050,000	$1,102,500
B8	Profit margin	Composite	10%	10%	10%
B9	Subtotal: avoided business loss due to lost revenue	B1*B3*B7*B8	$50,000	$52,500	$55,125
B10	Brand risk exposure	Composite	50%	50%	50%
Bt	Avoided or reduced crisis reputational damage due to crises and associated recovery costs	(B4+B9)*B10	$100,000	$101,250	$102,563
	Risk adjustment	↓20%			
Btr	Avoided or reduced crisis reputational damage due to crises and associated recovery costs (risk-adjusted)		$80,000	$81,000	$82,050
	Three-year total $243,050		**Three-year present value $201,315**		

INCIDENT COST SAVINGS BY REDUCING DUPLICATIVE OR UNNECESSARY EFFORT

Evidence and data. Interviewees described historical situations where leadership, board members, or other personnel with appropriate spending authority would engage internal or external resources to respond to external crises or critical events without the corporate security team's involvement.

- Interviewees noted that when leadership learned of potential incidents through the news media and not from corporate security, they would frequently act immediately.
- Trust of corporate security's ability to act quickly and decisively was not as high before using Dataminr.
- Duplicative or unnecessary actions taken included engaging external legal, public relations, and marketing services as well as external firms that deal with corporate security risk and recovery.

"Dataminr gives us instant, real-time access to information on incidents so that we can provide leadership with salient information with an action plan in advance of them even hearing about it. Our relationship has evolved to the point where they trust our ability to respond to events and no longer act without talking to us. I have sought to be the trusted advisor for five CEOs in my career; by enabling me to provide information that can't be found anywhere else, Dataminr has made it easier to get that trust."

CSO, data analytics and technology

"Dataminr helps us as a company by eliminating any perceptions that security moves slow. We are at a point where our leadership will not take any security-related actions on their own due to our very close relationship with them as their trusted advisors around all security and health and safety matters."

Global head of security operations, enterprise software

Modeling and assumptions. Based on customer interviews, Forrester estimates the following for the composite organization:

- The organization has 25 annual incidents that require corporate security action but do not require significant internal or external actions.
- Ten percent of these incidents include some level of unnecessary escalation initiated by other internal organizations.
- The median average cost per unnecessary activity is $15,000.

Risks. Risks that could impact the realization of this benefit include:

- The level of brand risk exposure, real or perceived, affects the need to act quickly.
- The corporate culture may lead to more or less reactionary activity.
- The cost variance differed significantly across interviewed organizations. It could be more than double for some organizations.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of more than $79,000.

Incident Cost Savings By Reducing Duplicative Or Unnecessary Effort

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Incidents with required action but no need for corporate escalations	Composite	25	25	25
C2	Percentage of incidents previously first identified by noncorporate security leadership, leading to unnecessary engagement	Interviews	10%	10%	10%
C3	Incidents with unnecessary engagement by legal, communications, or outside consultancies	C1*C2	2.5	2.5	2.5
C4	Average cost per incident with unnecessary engagement	Interviews	$15,000	$15,000	$15,000
Ct	Incident cost savings by reducing duplicative effort or unnecessary effort	C3*C4	$37,500	$37,500	$37,500
	Risk adjustment	↓15%			
Ctr	Incident cost savings by reducing duplicative effort or unnecessary effort (risk-adjusted)		$31,875	$31,875	$31,875
	Three-year total: $95,625			**Three-year present value: $79,268**	

“There is no one-stop shop for corporate security. Dataminr is our go-to for first alerting, while we use Dataminr and other tools for investigations and other tools for case management and mass messaging. I would say that Dataminr has also helped us reduce the number of tools we need to use for individual events.”

Global security center manager, technology

AVOIDED CORPORATE SECURITY LABOR AND REDUCED SOFTWARE COSTS

Evidence and data. Interviewees described reducing their use of other software tools as well as saving analyst time by receiving more relevant alerts. They also noted balancing central and regional security team labor to meet growing demands, including 24/7 coverage and global exposures.

- More immature corporate security teams were able to add fewer tools due to Dataminr’s early alerts, global coverage, translations, and ongoing alert updates that increase context about an incident, as well as personalized alert settings that minimize false positives.
- More mature corporate security teams and large enterprises continue to consider eliminating other

tools but have mostly reduced utilization of these tools.

- Interviewees described how Dataminr provides focused alerts, saving analysts' time both in the volume of alerts that they have to review and by reducing unnecessary analysis due to false-positive alerts.
- Dataminr supports the expanded interest in 24/7 coverage with its alerts based on AI algorithms. The technology organization's global security manager said, "Our security centers would need 24/7 teams doing web scraping to meet our global and early response requirements."
- Most corporate security teams have deployed Dataminr alerts to regional security teams, allowing the central team to tune their alert settings to avoid receiving alerts that need to be handled at a more local level.

Modeling and assumptions. Based on customer interviews, Forrester estimates the following for the composite organization:

- The composite organization reduces annual software costs by approximately 10%, or $50,000.
- One FTE is avoided due to alert-related labor productivities and Dataminr's AI support of 24/7 coverage, as well as the ability to reduce how many analysts need to work on certain local incidents.

> **"I pay close attention to the alerts that I get because we did the front-end work to make sure I'm only getting and seeing things that might be relevant."**
>
> *Head of intelligence, travel and hospitality*

Risks. Risks that could impact the realization of this benefit include:

- Corporate security organizations may be wary about reducing or eliminating components of their toolset.
- Some organizations may not need 24/7 coverage and may not be large enough to need regional security teams.
- Corporate cultures or strategies may not support having regional teams.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $391,057

Avoided Corporate Security Labor And Reduced Software Costs					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	Elimination or reduction in use of other corporate threat intelligence software	Interviews	$50,000	$50,000	$50,000
D2	Avoided increased central organization staffing to provide 24/7 coverage and support noncorporate-level regional and local needs	Composite	1.00	1.00	1.00
D3	Annual fully loaded corporate security FTE salary	TEI standard	$135,000	$135,000	$135,000
D4	Subtotal: additional corporate security labor cost to provide 24/7 coverage and improved noncorporate-level regional and local needs	D2*D3	$135,000	$135,000	$135,000
Dt	Avoided corporate security labor and reduced software costs	D1+D4	$185,000	$185,000	$185,000
	Risk adjustment	↓15%			
Dtr	Avoided corporate security labor and reduced software costs (risk-adjusted)		$157,250	$157,250	$157,250
	Three-year total: $471,750			**Three-year present value: $391,057**	

AVOIDED LABOR COST TO PROVIDE NECESSARY EARLY WARNINGS AND EMERGING-MARKET SOURCES NOT AVAILABLE IN OTHER SOLUTIONS

Evidence and data. Interviewees with multiple tools called out capabilities within Dataminr that don't exist in any other tool, which they consider essential for them to effectively reduce corporate risk.

- Dataminr notified corporate security teams 30 minutes to several hours ahead of other tools about incidents that involve employee safety or have major brand reputation implications. Interviewees wanted these categories of incidents provided on a near-real-time basis.
- Interviewees consider Dataminr's translation capability to be effective, allowing coverage of global incidents without language barriers.
- Interviewees whose organizations have exposures in emerging-market countries realized that Dataminr provided them with alerts from sources not used by their other tools.

"Dataminr caught a major international incident off of a single tweet [in a foreign language and from an emerging-market country]. We were able to piece together that it was true via an industry-specific tool that we use. We activated a team within 5 minutes of the tweet. The team was able to work on things for over an hour before mainstream media started covering it. Our team having that much time to prepare before it became public knowledge was very valuable."

Crisis and risk manager, manufacturing

Modeling and assumptions. Based on customer interviews, Forrester estimates the following for the composite organization:

- Without Dataminr, 20% of an FTE's time is allocated to produce alerts identifying life-threatening or significant brand reputation risks on a near-real-time basis.
- Without Dataminr, 20% of an FTE's time is allocated to obtaining data and producing alerts in areas where there is inadequate coverage from other tools.

Risks. Risks that could impact the realization of this benefit include:

- Risk to employees and brand reputation will vary per organization.
- An organization's presence in emerging markets or areas with limited visibility will vary.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of more than $99,000.

Avoided Labor Cost To Provide Necessary Early Warnings And Emerging-Market Sources Not Available In Other Solutions

Ref.	Metric	Source	Year 1	Year 2	Year 3
E1	Labor (FTEs) to collect required near real-time data to support early action	Composite	0.20	0.20	0.20
E2	Labor (FTEs) to access, collect, translate, and consolidate emerging-market data not available in other TI solutions	Composite	0.20	0.20	0.20
E3	Annual fully loaded labor cost	TEI standard	$125,000	$125,000	$125,000
Et	Avoided labor cost to provide necessary early warnings and emerging-market sources not available in other solutions	(E1+E2)*E3	$50,000	$50,000	$50,000
	Risk adjustment	↓20%			
Etr	Avoided labor cost to provide necessary early warnings and emerging-market sources not available in other solutions (risk-adjusted)		$40,000	$40,000	$40,000
	Three-year total: $120,000			**Three-year present value: $99,474**	

UNQUANTIFIED BENEFITS

Additional benefits that customers experienced but were not able to quantify include:

- **Saving human life.** Most interviewees spoke of specific events where Dataminr alerts led to early action that they considered significant toward protecting employees, customers, or other workers. The travel and hospitality head of intelligence spoke of four events that occurred in the seven days prior to the interview that could have negatively affected employees or customers.

  The global head of security operations for an enterprise software organization shared: "For incidents where we have to react quickly, we can react much earlier than we reacted before. There was a terror attack in [a foreign country], in a hotel complex where we had our office. A Dataminr alert came out 30 minutes before any of our other intelligence sources. We mass-notified employees there well before 30 minutes, and our employees got out safely."
- **Maintaining an employee-first reputation.** The corporate security team's actions to protect employees demonstrated a commitment to employees' well-being that was recognized internally. Although protecting employees

couldn't be directly associated with employee retention, some interviewees believed that their good work helped with employee satisfaction with their organization.

- **Securing the trust of corporate leadership.** Interviewees noted that their relationship with corporate leadership improved because of their ability to act quickly and decisively using Dataminr.

"Dataminr enables me to write an 'All clear' or 'Covered' message to key internal people outside my team before they get a chance to get worried. It's very important that we as a security organization are faster on these items than our executive team because when they have this information before they even realize there was an incident, it builds trust in our security organization."

Global head of security operations, enterprise software

- **Proactive action that keeps the company out of the limelight reduces future guilt by association.** Many benefits will increase over time by preventing the repeated association of the company or product with crises and critical events. Interviewees noted that they want to minimize any attention to their brand, product, or organization when an incident occurs.
- **Partnering with a strong customer success team.** Interviewees called out the Dataminr customer success and account management teams, support functions that are included in the base contract, as crucial partners in ensuring their success. They worked to understand interviewee's goals and needs, personalize account settings, provide training, assess and improve performance, and share best practices.

  The global security center manager for a technology organization shared: "Dataminr is easy to learn and made even easier by the diligent efforts of the customer success team. They're always checking in [and are] available for training, and they provide us with numerous resources."
- **Monitoring the COVID-19 pandemic.** Some of the interviewed customers used Dataminr's COVID-19 tracking, where Dataminr associated spikes in social media posts in areas just prior to COVID-19 flare-ups. At times, this proved useful in making early decisions, but in general it let customers know where to focus their attention.

  The global security center manager at a technology company told Forrester: "Dataminr has helped us during the pandemic, especially for COVID monitoring. Dataminr quickly recognized that their customer base was going to deal with a very new problem set, so they quickly built out algorithms to understand the COVID space and the reporting needs for this pandemic. It was so easy to just say, let's click on 'coronavirus' as a topic-based search and the information started being fed to us. Honestly, global security ended up being the leader in all of our COVID response because we were able to provide actionable information. We have the intelligence rigor, intelligence, and analysis support to help build and execute on some of these plans."

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Dataminr and later realize additional uses and business opportunities, including:

- **Organizing the corporate security team.** Interviewees spoke of the flexibility of organizing their corporate security team. Larger organizations have central, regional, local and mobile team members while others are able to meet expectations with a highly centralized organization.
- **Expanding to other teams.** Dataminr was employed for numerous other use cases such as compliance, tracking government policy changes, supply chain risk, and identifying employee disenfranchisement. The interviewees could not speak to the value of uses by other departments.

"Reputationally within the company, Dataminr is a winner. We work with operational folks, corporate communications, legal — all these departments — because we have great information coming in, in a timely manner. A lot of other functions have grown dependent on our expertise."

Head of intelligence, travel and hospitality

- **Goodwill at special events.** Interviewees described expanding their use of Dataminr to executive protection of VIP customers and leadership at special events. Providing these services likely provided additional value to the organization, either directly or indirectly.
- **Using the open API for additional automation and supporting other focused use cases.** Interviewees integrated Dataminr data into other security and risk management systems, allowing automation opportunities and supporting workflow automation.

  The global security center manager for a technology company shared: "I have been in this space for a long time. There is no silver bullet. There isn't an application out there to satisfy every information intelligence collection requirement that a company has. We have unique needs, and we see it as a partnership. Dataminr has stepped up to navigate this really complicated space. The API, for example, has allowed us to take advantage of the fact that the computer can move much faster than a human can in evaluating information coming in, and we are automating some of these processes."

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Ftr	Setup, training, and licensing costs	$23,000	$74,750	$81,650	$88,550	$267,950	$224,963
	Total costs (risk-adjusted)	$23,000	$74,750	$81,650	$88,550	$267,950	$224,963

SETUP, TRAINING, AND LICENSING COSTS

Evidence and data. Interviewees spoke of a short, professional implementation process.

- Utilizing Dataminr's customer success team, customers received support with personalized account settings and were provided the training, documentation, and other resources to use Dataminr effectively. These customer success services and support were included in the annual licensing subscription fee.
- Interviewees spoke of the ease of use of Dataminr's user interface.
- The composite organization did not incur any outside professional services costs to utilize Dataminr.
- The customer success team supported setting up user settings as well providing advice toward API integration and tool use.

Modeling and assumptions. Based on customer interviews, Forrester estimates the following for the composite organization:

Risks. The cost can vary based on:

- The size and scope of the deployment across teams, business units, geographies, etc.
- The use cases and usage mix within the solution.
- Integration requirements with other tools.

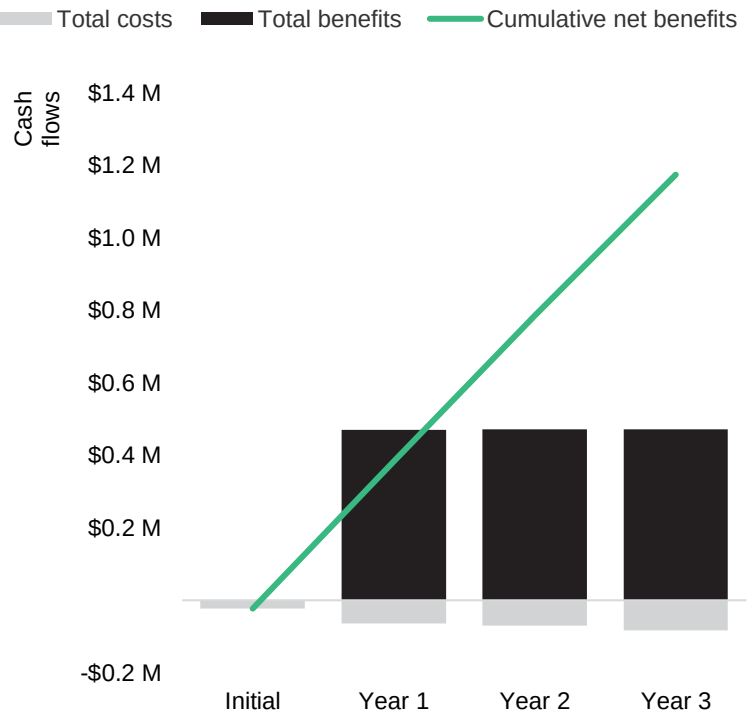
Results. To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $224,963.

Setup, Training, And Licensing Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
F1	Setting up profiles, setting up data APIs, and training	Composite	$20,000		$1,000	$2,000
F2	Licensing and customer success services	Composite		$65,000	$70,000	$75,000
Ft	Setup, training, and licensing costs	F1+F2	$20,000	$65,000	$71,000	$77,000
	Risk adjustment	↑15%				
Ftr	Set\up, training, and licensing costs (risk-adjusted)		$23,000	$74,750	$81,650	$88,550
	Three-year total: $267,950			**Three-year present value: $224,963**		

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($23,000)	($74,750)	($81,650)	($88,550)	($267,950)	($224,963)
Total benefits	$0	$470,125	$471,125	$472,175	$1,413,425	$1,171,497
Net benefits	($23,000)	$395,375	$389,475	$383,625	$1,145,475	$946,534
ROI						421%
Payback (months)						<6

Appendix A: Total Economic Impact

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.

TOTAL ECONOMIC IMPACT APPROACH

Benefits represent the value delivered to the business by the product. The TEI methodology places 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.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV Sources are calculated for each total cost and benefit estimate. NPV Sources in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value Sources of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

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.

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.

RETURN ON INVESTMENT (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

DISCOUNT RATE

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

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.

Appendix B: Endnotes

[1] 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.


FORRESTER®