TOTAL ECONOMIC IMPACT

The Total Economic Impact™ Of Immersive

A FORRESTER TOTAL ECONOMIC IMPACT STUDY COMMISSIONED BY IMMERSIVE , JANUARY 2026

COST SAVINGS AND BUSINESS BENEFITS ENABLED BY THE IMMERSIVE ONE PLATFORM

FORRESTER®

Table Of Contents

Executive Summary

The Immersive One platform allows organizations to continuously prove, upskill, benchmark, and report workforce cyber resilience skills across many roles, providing actual performance data (rather than completion percentage) to organizations and their regulators at scale. Investing in employee cyber resilience across several roles yields more internally produced cybersecurity talent, fewer external hires, better attrition rates, and a better organizational security posture that is resilient in an ever-changing threat landscape.

Forrester research states: "Forrester's Security Survey, 2025 found that 87% of security decision-makers hiring early career and midlevel or senior cybersecurity practitioners consider it important to prioritize demonstrable skills. Demand for skilled mid- to senior-level security staff especially will continue to outweigh supply for the foreseeable future as certification bodies and higher education institutions struggle to keep up with the breakneck pace of AI adoption, forcing security and risk leaders to look within their own organizations to find and develop nascent or previously hidden cybersecurity talent. Cybersecurity skills and training (CS&T) platforms enable this shift to a skills-based talent management practice that values demonstrable skills over point-in-time-based cybersecurity certifications."[1]

Immersive One is a unified SaaS platform that equips organizations to prove, improve, benchmark, and report their cyber resilience. Immersive commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying the Immersive One platform.[2] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Immersive on their organizations.

327%

Return on investment (ROI)

$2.2M

Net present value (NPV)

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed six decision-makers with experience working with Immersive. For the purposes of this study, Forrester aggregated the experiences of the interviewees and combined the results into a single composite organization, which is an industry agnostic organization with ~4,200 Immersive users and $40 billion annual revenue.

By investing with Immersive, the interviewees noted that their organizations are in a position to scale cyber resilience exercises across many teams within the organization, improving security preparedness and overall security posture while benchmarking skills, proving readiness, and closing resilience gaps.. Investing in cybersecurity talent at scale with Immersive fosters the development of homegrown talent, reducing attrition rates and the need for external hires.

Key Findings

Quantified benefits. Three-year, risk-adjusted present value (PV) quantified benefits for the composite organization include:

- **Improved cybersecurity attrition rate by 3%.** Investing in the composite organization's cybersecurity staff via cyber resilience training on Immersive engaged staff in ways that previous efforts did not, allowing for career advancement and opportunities that improve cybersecurity staff retention and reduce the composite organization's costs associated with attrition.
- **Avoided up to four cybersecurity hires annually.** Immersive One engages the composite organization's cybersecurity staff more than previous efforts, allowing it to track skills attainment, set employees' career paths, and identify talent within cybersecurity teams that previously went unnoticed or underutilized, allowing for more frequent promotions of these personnel. Through upskilling and cybersecurity skills development, the composite organization hires external talent less frequently.

- **Reclaimed 2,400 developer hours through secure coding upskilling.** The Immersive One platform offers labs aimed specifically at developers to instill best practices for secure coding into software development lifecycles (SDLCs). Through more consistent developer engagement with Immersive and adopting these practices, the composite organization's developers realize fewer hours of vulnerability remediation and coding rework by discovering or avoiding these issues early in the SDLC.
- **Saved more than $100,000 annually on legacy cybersecurity training costs.** By investing with Immersive, the composite organization reduces some of the costs previously associated with cyber resilience training across cybersecurity personnel, developers, executives, and the wider workforce. The composite scales training opportunities that were previously offered to fewer, select participants across the entire organization.
- **Improved organizational security posture, reducing quantifiable risk by more than $250,000 over three years.** By implementing Immersive's crisis simulations and exercises across the composite organization's personnel, its security posture improves through better preparedness and response against the latest threats, more secured applications, and security awareness across the wider workforce.

Unquantified benefits. Benefits that provide value for the composite organization but are not quantified for this study include:

- **Higher cybersecurity awareness within the organization.** By leveraging Immersive One, security culture at the composite organization is more top-of-mind for users in many roles. Beyond the annualized risk exposure quantified for this report, the improvement to security posture may help the organization avoid major security breaches that may result in fines or reputational damage.
- **Employee experience and upskilling.** Immersive One engages cybersecurity personnel in a way that previous options did not, driving higher engagement, skills development, and ultimately higher job satisfaction and upskilling for promotions.
- **Security framework and compliance standard alignment.** Immersive One allowed the composite organization to map skills and capabilities to security frameworks and meet compliance standards.
- **Hiring and onboarding skills assessments.** The composite uses Immersive One as part of its hiring process, ensuring it recruits the most qualified candidates, potentially reducing onboarding costs, and further improving attrition.
- **Shorter SDLCs.** By leveraging Immersive One across the composite organization's developer bases, developers spend less time remediating vulnerabilities further in the SDLC, not only saving developer time but also accelerating software delivery to internal clients and customers alike.

Costs. Three-year, risk-adjusted PV costs for the composite organization include:

- **Subscription fees for Immersive One of $250,000 annually.** The composite organization pays for its Immersive products based on several factors, including the number of employees exercised (and their roles); frequency and access to labs and exercises; and the specific types of labs, exercises, and simulations.
- **Internal personnel effort of $16,500 annually.** The composite organization dedicates internal personnel effort to maintain the Immersive relationship and ensure its users maximize their access (e.g., managing user and team access, interfacing with Immersive's support team, planning simulations for cybersecurity teams).

The financial analysis that is based on the interviews found that a composite organization experiences benefits of $2.9 million over three years versus costs of $674,000, adding up to a net present value (NPV) of $2.2 million and an ROI of 327%.

> *"Immersive [One] as a suite of tools is increasing communication, collaboration, and skills in cybersecurity on different levels across the organization."*
>
> **Cybersecurity manager, insurance**

> *"Our Immersive relationship allows us to be fairer and more equitable with our hands-on cybersecurity opportunities while being able to track and report skills progress. We now have better assessments of our teams' knowledge and skill sets."*
>
> **VP of program management and strategic projects, managed services**

Key Statistics

327%

Return on investment (ROI)

$2.9M

Benefits PV

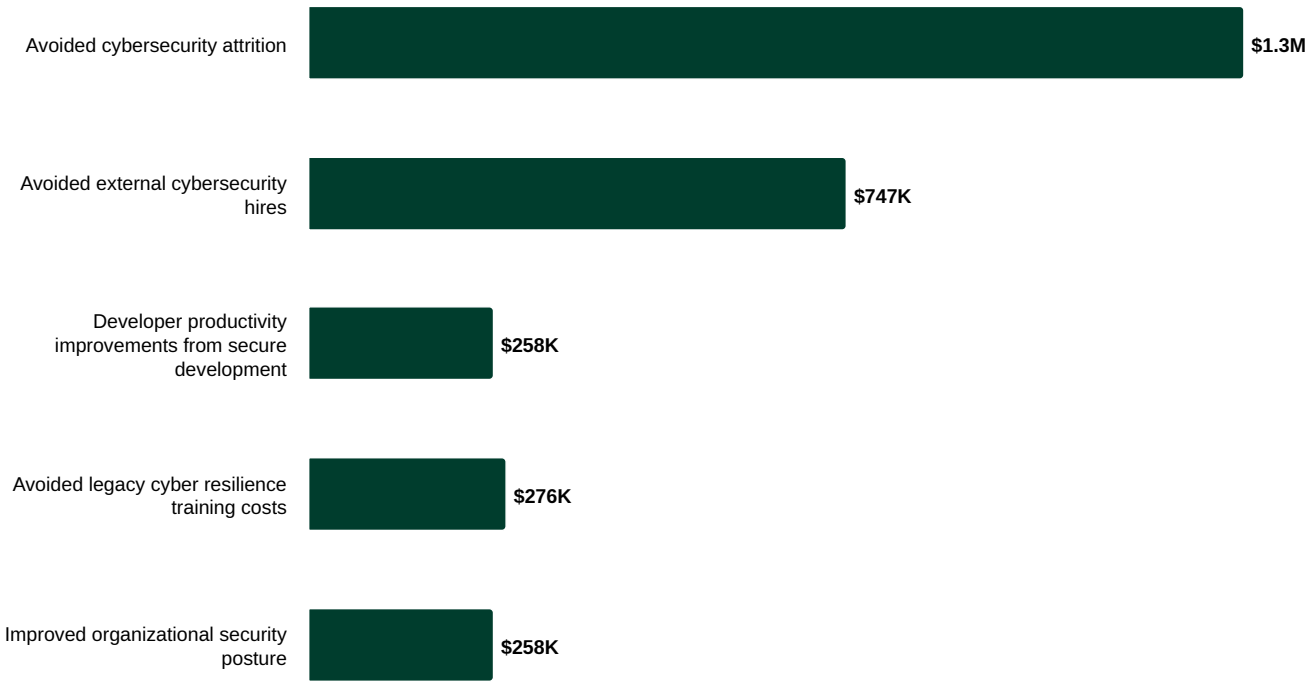
$2.2M

Net present value (NPV)

<6 months

Payback

Benefits (Three-Year)



The Immersive One Customer Journey

Drivers leading to the Immersive One investment

Interviews			
Role	**Industry**	**Region**	**Revenue**
Global lead, cybersecurity fusion center response and readiness	Banking	North America	~$81B
Cybersecurity education and awareness lead	Banking	Europe	~$52B
Cybersecurity manager	Insurance	Europe	~$60B
Director of cyber threat management	Insurance	North America	~$27B
VP of program management and strategic projects	Managed services	North America	~$600M
Principal, cybersecurity	Telecommunications	North America	~$124B

Key Challenges

Interviewees noted how their organizations struggled with common challenges, including:

- **Understanding the latest threats and vulnerabilities.** Before working with Immersive, interviewees acknowledged blind spots in their capabilities around new threats or vulnerabilities, as they "didn't know what they didn't know." The cybersecurity education and awareness lead at a global bank explained: "What did our threat hunters need to be looking for? What did our SOC analysts need to be aware of? We needed this to get our [response] to be as real time as possible." As such, several interviewees noted that their CISOs directly mandated exploring partners such as Immersive.
- **Disparate cyber resilience training methods and programs across the organization.** Interviewees explained consistency challenges with ensuring that cybersecurity personnel had access to simulations and cyber resilience training. They noted that training was often done at the team level, resulting in excess cost, an inability to measure skills and competency across the organization, and difficulty adhering to cyber resilience frameworks.
- **Difficulty measuring or assessing staff competency levels.** Prior to the investment with Immersive, interviewees noted that previous cyber resilience training efforts did not give their teams a way to assess skills consistently among cybersecurity staff, leaving higher potential staff more likely to churn out or remain anonymous within the broader cybersecurity team via a lack of engagement or promotion opportunities. In turn, interviewees' organizations had to look outside for cybersecurity talent more often.
- **Costly, per-employee training expenditure that didn't scale.** Several interviewees noted that investing in their organization's personnel often meant ad hoc, per-employee investment in training or certifications (e.g., SANS Institute) that forced managers to choose among staff to determine who received the training. However, selection factors for these courses were often inconsistent. Furthermore, program costs often forced organizations to limit the number of staff enrolled, further bottlenecking broader organizational skills development. The interviewee at the managed services organization added, "There was no true way for us to be equitable with these opportunities given budget." Some interviewees explained that their organizations developed (or attempted to develop) internal programs to deliver cyber resilience training to more cybersecurity personnel for hands-on learning, though these efforts fell short given the internal expertise, personnel hours, and agility (in the face of new threats) to be viable.
- **Connecting the right cyber resilience exercises with the right internal audiences.** Some interviewees noted the challenges associated with finding, developing, and/or maintaining cyber resilience training specific to each user group that appropriately built role-specific competencies and engaged users. For instance, the interviewee at the managed services firm noted the

need to nuance cyber resilience training for several sub-roles within the larger cybersecurity team, including (but not limited to) threat hunting, incident response, and security preparedness. With Immersive, the interviewee noted that this was now possible. The interviewee at the North American insurance organization explained that securing application development by instilling secure development best practices was a focus. They explained, "We were looking to broaden training and tailor it to the needs of the developer."

> *"We've always had an external training budget, but it was a bit of a scattershot. Most of it went towards in-person SANS-type training, which is great, but also very expensive. And now that we've grown 40%, that just doesn't scale anymore."*
>
> **VP of program management and strategic projects, managed services**

> *"We had a huge library internally, but keeping modules updated took too much effort, especially when it comes to training, documentation, exercises, and competency tests. And not just around security, but the entire business. It was a major undertaking. It's even more challenging just because of the very dynamic nature of cybersecurity. We may have some expertise, but we didn't have the business commitment to fully build out and sustain this program. We needed a partner."*
>
> **Principal, cybersecurity, telecommunications**

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 interviewees' organizations, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

- **Description of composite.** The composite organization is a global, $10 billion, industry-agnostic organization with 40,000 employees (including 1,000 developers and 200 cybersecurity professionals). The composite organization has a financial services division dealing in sensitive customer information, necessitating the proof of cyber resilience capabilities and an ongoing effort to improve security posture and readiness against the latest cyber threats and vulnerabilities.
- **Deployment characteristics.** Among the organization's employees, ~4,200 are enabled with Immersive One cyber resilience training. This includes 200 cybersecurity staff, 1,000 developers, and 3,000 wider workforce employees including the entire executive team. The annual investment with Immersive includes:
  - Hands-on labs: Each user group receives unlimited access to labs relative to their roles.
  - Cyber range exercises: All cybersecurity personnel have access to a cyber range exercise once per quarter, completed in teams.
  - Crisis simulations: Each user has access to crisis simulations (monthly) to test non-technical decision-making against crisis response playbooks.
  - Workforce exercises: The wider workforce has unlimited access to micro exercises to gauge the wider risk profile of the business, with targeted labs assigned based on performance to address improvement areas.

KEY ASSUMPTIONS

- $10 billion revenue
- 200 cybersecurity personnel on Immersive
- 1,000 developers on Immersive
- 3,000 wider workforce and executive team on Immersive

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	Avoided cybersecurity attrition	$330,000	$660,000	$660,000	$1,650,000	$1,341,322
Btr	Avoided external cybersecurity hires	$116,875	$350,625	$467,500	$935,000	$747,262
Ctr	Developer productivity improvements from secure development	$103,680	$103,680	$103,680	$311,040	$257,837
Dtr	Avoided legacy cyber resilience training costs	$110,880	$110,880	$110,880	$332,640	$275,742
Etr	Improved organizational security posture	$103,632	$103,632	$103,632	$310,895	$257,717
	Total benefits (risk-adjusted)	$765,067	$1,328,817	$1,445,692	$3,539,575	$2,879,880

Avoided Cybersecurity Attrition

Evidence and data. Beyond the security posture factors that mandated the organizations' investments with Immersive One, interviewees explained to Forrester that investing in their cybersecurity staff via cyber resilience training engaged staff in ways that previous efforts did not, allowing for career advancement and opportunities that improved cybersecurity staff retention and reduced organizational attrition costs.

- Prior to the Immersive relationship, the interviewee at the managed services firm explained that their organization invested in its cybersecurity staff (via certification or hands-on training) as a retention tool. While this was very effective from a retention standpoint, growth in the size of the team and the cost associated with these programs meant that it could not be scaled much further. By investing with Immersive One, these types of hands-on simulation opportunities can now be provided to the entire cybersecurity team. The interviewee noted that since then, "regrettable" churn on the team has decreased by 7%, most of which is attributable to investing in their employees at scale with Immersive.
- The interviewee at the European-headquartered bank noted that using Immersive in the recruitment process to gauge skills competency prior to hiring has ensured they fill roles with personnel of the appropriate skill sets, potentially reducing churn.
- The same interviewee explained that transparent career pathways through skills development on Immersive One helped support employee development, contributing to low attrition among the cybersecurity teams in the organization compared to the industry.

Modeling and assumptions. For the composite organization, Forrester makes the following assumptions:

- There are 200 cybersecurity professionals across the organization's cybersecurity teams.
- A 12% pre-Immersive One annual attrition rate for these cybersecurity professionals, which improves to 9% with Immersive.
- In Year 1 of the analysis, the organization fills only half of its cybersecurity openings, as hiring for these roles may take up to six months. By Years 2 and 3 of the analysis, it fills each open role annually.
- The average fully burdened annual salary for a cybersecurity hire is $125,000.
- The cost to hire and onboard a cybersecurity professional is 110% of the annual salary. It should be noted that assumptions for the cost of attrition range from 100% of the annual salary to more than 125% of the annual salary, depending on the seniority of the role.

Risks. This benefit will vary based on:

- An organization's historical attrition rate for cybersecurity personnel.
- The ability for an organization to recruit and onboard cybersecurity personnel.

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 $1.3 million.

3%

Improvement to cybersecurity personnel attrition rate

> *"Immersive has allowed us to really build out those career pathways, which has influenced attrition in a favorable direction."*
>
> **VP of program management and strategic projects, managed services**

Avoided Cybersecurity Attrition					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Total cybersecurity personnel	Composite	200	200	200
A2	Cybersecurity personnel attrition rate (pre-Immersive)	Composite	12%	12%	12%
A3	Cybersecurity personnel attrition rate (with Immersive)	Interviews	9%	9%	9%
A4	Improved cybersecurity attrition rate with Immersive	A2-A3	3%	3%	3%
A5	Avoided annual cybersecurity personnel attrition (rounded)	A1*A4	6	6	6
A6	Cybersecurity openings filled annually	Composite	50%	100%	100%
A7	Fully burdened annual salary for cybersecurity personnel (rounded)	Composite	$125,000	$125,000	$125,000
A8	Average cost to hire and onboard cybersecurity FTEs	TEI methodology	110%	110%	110%
At	Avoided cybersecurity attrition	A5*A6*A7*A8	$412,500	$825,000	$825,000
	Risk adjustment	↓20%			
Atr	Avoided cybersecurity attrition (risk-adjusted)		$330,000	$660,000	$660,000
	Three-year total: $1,650,000			**Three-year present value: $1,341,322**	

Avoided External Cybersecurity Hires

Evidence and data. Among the organizations that invested with Immersive One, interviewees explained that both engagement (percentage of employees who completed at least one lab or exercise) and time spent on Immersive One-related activities were both considerably higher than those of previous training efforts or programs. The ability for the organization to track employee engagement and prove competency on Immersive One allowed these organizations to identify talent within cybersecurity teams that previously went unnoticed or underutilized, allowing for more frequent promotions of these personnel and a reduced burden on the organizations to hire required talent and skills from outside the organization.

- Immersive One allows the cybersecurity teams at the managed services organization define, develop, and track skill requirements and attainment for each role of seniority, resulting in clear pathways for internal skills development and promotions and potentially avoided external hiring. The interviewee summarized: “With Immersive One, we have defined our competency matrix with what we expect each tier of [cybersecurity role] should be able to do. For our top tiers, for example, we need to make sure that they can do threat hunting, that they can do the deep forensic analysis. Immersive One gives us the consistent methodology to develop and the proof that we need.”
- The same interviewee relayed an anecdote where a recent simulation performance from an unassuming team member helped the team discover the depth of knowledge this individual (unknowingly) possessed. They have recently been promoted (reducing the need for an external hire) with a high potential employee career path in front of them.
- Interviewees at several organizations noted that Immersive allowed them to formalize cybersecurity career paths based on skills development pathways and provided the ability to prove them. The interviewee at the North American bank summarized: “We’ve developed multiple pathways with Immersive [One] for development and upskilling of our [cybersecurity] workforce.”
- Some interviewees said that their organizations have been able to hire internal personnel with little to no experience in cybersecurity through upskilling on Immersive One, avoiding the need to hire externally at a greater cost to their organizations, while more experienced staff have moved to other roles or been promoted. The interviewee at the European insurance organization also noted: “There have been many sideways moves [in cybersecurity] generated off communities fostered by Immersive that have brought people closer. Some of these people wouldn’t have seen or heard about those jobs previously.”

Modeling and assumptions. For the composite organization, Forrester makes the following assumptions:

- There are 200 cybersecurity professionals across the organization’s cybersecurity teams.
- The organization avoids 1% to 2% of its external skills requirement through internal upskilling/promotions with Immersive One.
- In Year 1 of the analysis, the organization fills only half of its cybersecurity openings, as hiring for these roles may take up to six months. By Years 2 and 3 of the analysis, it fills each open role annually.
- The average fully burdened annual salary for a cybersecurity hire is $125,000.
- The cost to hire and onboard a cybersecurity professional is 110% of their annual salary.

Risks. This benefit will vary among organizations based on:

- The skill and capacity of an organization’s cybersecurity personnel related to their ability to develop new skills.
- The preexisting cybersecurity skills within an organization related to the need to hire externally.
- An organization’s industry related to its cybersecurity skills requirements.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $747,000.

4 cybersecurity professionals

Avoided hires resulting from internal skills development on Immersive

> *"There are certainly some people who have gotten jobs within our cybersecurity office who had no prior experience in cybersecurity. They just upskilled on Immersive."*
>
> **Cybersecurity manager, insurance**

Avoided External Cybersecurity Hires					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Total cybersecurity personnel	A1	200	200	200
B2	Annual cybersecurity hiring requirement avoidable through internal upskilling	Interviews	1.0%	1.5%	2.0%
B3	Required external hires (rounded)	B1*B2	2	3	4
B4	Cybersecurity openings filled annually	Composite	50%	100%	100%
B5	Fully burdened annual salary for cybersecurity personnel (rounded)	Composite	$125,000	$125,000	$125,000
B6	Average cost to hire and onboard cybersecurity FTEs	TEI methodology	110%	110%	110%
Bt	Avoided external cybersecurity hires	B3*B4*B5*B6	$137,500	$412,500	$550,000
	Risk adjustment	↓15%			
Btr	Avoided external cybersecurity hires (risk-adjusted)		$116,875	$350,625	$467,500
	Three-year total: $935,000			**Three-year present value: $747,262**	

Developer Productivity Improvements From Secure Development

Evidence and data. The Immersive One platform offers labs aimed specifically at developers to instill best practices for secure coding into SDLCs. Through more consistent developer engagement with Immersive One and adoption of these practices, organizations' developers realize fewer hours of vulnerability remediation and coding rework by discovering or avoiding these issues early in the SDLC (and especially prior to production).

- The interviewee at the North American bank explained that Immersive One's developer-focused training modules allow developers to train on best practices for avoiding late SDLC or production vulnerabilities, greatly reducing risk exposure for the organization while avoiding developer remediation hours.
- Given the utmost importance of secure development practices at the North American insurance organization, the interviewee explained that they mandate developers to complete labs on Immersive One to retain access to code repositories. The interviewee summarized: "In an application where a flaw is found in production, it costs a whole lot of time and money to fix it compared to preventing it [in the first place]. We're seeing far fewer flaws in applications developed by the folks that we are training on Immersive. That is also a huge risk reduction, as well." The interviewee estimated that training on Immersive One (among other optimizations) has contributed to reducing the amount of time developers spend on vulnerability remediation by nearly 50%.

Modeling and assumptions. For the composite organization, Forrester makes the following assumptions:

- Eighty percent of the organization's 1,000 developers leverage Immersive One and exercises annually.

- Each developer spends an average of 60 hours annually on software remediation work for vulnerabilities discovered later in the SDLC.
- It can avoid an average of 5% of these hours with best practices and secure coding practices honed on Immersive.
- The average fully burdened hourly rate for a developer is $72.
- Forrester applies a 75% productivity recapture rate, as not all reclaimed hours will be used for value-adding work.

Risks. This benefit will vary among organizations based on:

- The number of developers within the organization leveraging Immersive One.
- An organization's typical SDLC as it relates to vulnerabilities requiring remediation in production, and the time required to remediate these issues.
- The skill and capacity of an organization's developers to implement Immersive-driven learnings into their SDLCs.

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 $258,000.

3 hours of remediation time

Per developer SDLC savings attributable to Immersive

> *"Developer-specific training on Immersive and the high interactivity of these modules drive high adoption among the developers, which helps vulnerability reduction."*
>
> **Global lead, cybersecurity fusion center response and readiness, banking**

> *"Immersive training helps us meet that regulatory regime and deliver a secure product by enabling our development team with the knowledge to write secure code, which ultimately translates into risk reduction."*
>
> **Director of cyber threat management, insurance**

Developer Productivity Improvements From Secure Development					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Total developers	Composite	1,000	1,000	1,000
C2	Developer adoption rate	Composite	80%	80%	80%
C3	Average developer time spent on vulnerability remediation (hours)	Composite	60	60	60
C4	Reduction in remediation time with Immersive (with secure coding training)	Interviews	5%	5%	5%
C5	Avoided remediation time per developer (hours)	C3*C4	3.0	3.0	3.0
C6	Fully burdened hourly rate for a developer	Composite	$72	$72	$72
C7	Productivity recapture	TEI standard	75%	75%	75%
Ct	Developer productivity improvements from secure development	C1*C2*C5*C6*C7	$129,600	$129,600	$129,600
	Risk adjustment	↓20%			
Ctr	Developer productivity improvements from secure development (risk-adjusted)		$103,680	$103,680	$103,680
	Three-year total: $311,040			**Three-year present value: $257,837**	

Avoided Legacy Cyber Resilience Training Costs

Evidence and data. By investing with Immersive One, interviewees explained that their organizations were able to retire, reduce, or offset some of the costs previously associated with cyber resilience training across cybersecurity personnel, developers, executives, and their wider workforce. In particular, interviewees noted the ability for their organizations to save on costly, in-person training sessions that required both travel and limited participant selection. Furthermore, training opportunities that were previously offered to fewer select participants would now be scaled across the entire organization.

- The interviewee at the managed services organization explained that although their firm always had a cybersecurity training budget, it typically was spent on costly in-person certification sessions. However, given a 40% increase in the size of its already significant cybersecurity team in the last three years, this model would not scale with the new organization. Investing with Immersive One allowed the organization to avoid most of this in-person training budget (estimated at more than 70%, which nearly paid for the Immersive investment) through access to labs, crisis simulations, and cyber range exercises. In addition, with Immersive One, more cybersecurity professionals have access to hands-on training than in the previous model.
- The telecommunications organization dedicated significant personnel hours to curating a training and skills development program for its security personnel and wider workforce. However, the interviewee noted that the extreme effort required to keep modules updated and track employee skills quickly became untenable as they rolled out these skills development exercises to additional teams. By investing with Immersive One, the organization was able to reallocate five to ten full-time personnel to other endeavors within cybersecurity (depending on the year), as well as effort from content management personnel.
- Several interviewees' organizations gained additional savings by consolidating training across several vendors serving different employee populations. For instance, the interviewee from the North American bank said they saved "tons of money" by consolidating developer-focused training with cyber resilience training on Immersive.

Modeling and assumptions. For the composite organization, Forrester makes the following assumptions:

- The organization sends 3% of its 200 developers to an in-person cybersecurity training or certification program (e.g., SANS) annually (on average).

- It avoids 80% of this cost annually (on average) as Immersive One's labs, crisis simulations, and cyber range exercises allow for similar outcomes among the organization's cybersecurity professionals.
- It spends an average of $400 per cybersecurity professional on ongoing internal training expenditure, which is now avoidable with Immersive.

Risks. This benefit will vary among organizations based on:

- The typical annual expenditure on one-off cybersecurity training and certifications.
- An organization's current cyber resilience training programs or platforms related to the ability to reduce any of these costs on Immersive.
- The exact configuration of Immersive One products an organization contracts for.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $276,000.

$80K

Avoided annual recurring training expenses

> *"The scalability and 'rinse and repeat' nature of Immersive's crisis simulation tool is extremely beneficial. We have scenarios that we will use across several different audiences. Leveraging these scenarios that Immersive produces allows us to do that at scale without the heavy lift or prep work."*
>
> **Global lead, cybersecurity fusion center response and readiness, banking**

Avoided Legacy Cyber Resilience Training Costs					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	Total cybersecurity personnel	A1	200	200	200
D2	Cost per SANS training session	Composite	$9,000	$9,000	$9,000
D3	Percentage of cybersecurity personnel enrolled in SANS training (annual)	Composite	3%	3%	3%
D4	Average annual expense on SANS training	D1*D2*D3	$54,000	$54,000	$54,000
D5	Avoidable in-person training with Immersive relationship	Interviews	80%	80%	80%
D6	**Subtotal: Reduction of in-person training expenses**	**D4*D5**	**$43,200**	**$43,200**	**$43,200**
D7	Average per employee annual training program expenses	Interviews	$400	$400	$400
D8	**Subtotal: Avoided recurring training expenses**	**D1*D7**	**$80,000**	**$80,000**	**$80,000**
Dt	Avoided legacy cyber resilience training costs	D6+D8	$123,200	$123,200	$123,200
	Risk adjustment	↓10%			
Dtr	Avoided legacy cyber resilience training costs (risk-adjusted)		$110,880	$110,880	$110,880
	Three-year total: $332,640			**Three-year present value: $275,742**	

Improved Organizational Security Posture

Evidence and data. Interviewees noted that by implementing Immersive One's labs and exercises across their organizations' personnel, engagement with these products drove inherent improvements across their organizations' security posture. Cybersecurity personnel were able to prepare for and respond to the latest cyber threats and vulnerabilities, developers reduced the number of vulnerabilities making it to production, and the executive team and wider workforce were aware and prepared for the latest threats respective to their roles.

- Compared to other cyber resilience training programs that the managed services organization used or trialed in the past, this interviewee said that Immersive stood out for the depth and realism of the individual and team-based scenarios, providing a more actionable experience for cybersecurity staff should similar attacks occur. Penetration test catch rates improved from (at times) under 70% to 96% on average, speaking to a significant increase in security posture.
- Several interviewees commented on the speed with which Immersive delivers labs and simulations for the latest cyber threats and/or vulnerabilities, ensuring cybersecurity personnel at these organizations are in the best position to prepare for and respond to these threats. It was also noted that Immersive frequently refreshes the labs to remain current to the threat landscape and continue to engage users. The interviewee at the telecommunications organization noted that: "[Immersive] will have a training on a new attack vector within 48 hours that our staff can actually prepare with. [We] would take two months to develop it ourselves."
- As noted by several interviewees, Immersive allowed their organizations to track and assess the skills of their personnel in a regimented and consistent manner, ensuring proper skills development and contributing to a better security posture for their organizations.
- The interviewee at the North American bank summarized the scope of Immersive deployment and adoption at their organization, with more than 500,000 labs completed annually across the workforce and a significant adoption of crisis simulations among 100 users within cybersecurity.
- By rolling out and encouraging adoption of Immersive for the wider workforce, the interviewee at the European insurance organization explained the positive impact to security posture: "The bad actors are working faster than us. There's more

money in it for them, so they're always trying push the envelope and find new vulnerabilities. Even on the very lowest scale, having awareness on things like phishing across the entire organization with Immersive can make a huge difference."

- The ability to track and quantify skills attainment across an organization's cybersecurity teams on Immersive was cited as a major benefit by the interviewee at the European bank, who added: "We can quantify [skills attainment] that we can show to regulators to audit. From our executives' perspective, this alone makes the investment [with Immersive] worthwhile. This gives us the ability to say, 'Based on the number of threats, the type of threats, this is how deep our skills coverage is.' We can show the quality of skills attainment as well through pass rates. We can independently attest that knowledge with Immersive. It's not just a declaration. Immersive gives us quantifiable pieces so we can demonstrate what we're doing."
- The above interviewee also stressed the importance of Immersive's labs for their executive team members when it came to ensuring that security is top of mind in the decision-making process at the executive level.

Modeling and assumptions. For the composite organization, Forrester makes the following assumptions:

- The cumulative cost of data breaches for the composite organization is $4.4 million, based on Forrester's 2025 Security Survey.[3]
- The likelihood of the composite organization experiencing one or more security breaches annually is 68%.[4]
- Immersive can address 90% of the composite organization's breach vectors, resulting in an average annualized risk exposure addressable with Immersive of $2.4 million.
- Immersive reduces the organization's average risk exposure by 5% annually based on improvements to threat preparedness and response and a more secure SDLC.

Risks. This benefit will vary among organizations based on:

- An organization's size and industry related to the likelihood and costs associated with data breaches.
- The adoption of an organization's pre-Immersive cyber resilience programs and/or solutions related to the potential for improvements with Immersive.
- An organization's baseline security posture.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $258,000.

5%

Improvement to annualized risk exposure attributable to Immersive

> *"Immersive is always providing the latest and most up-to-date information on current threats via their labs so our teams can best prepare to mitigate those threats."*
>
> **Global lead, cybersecurity fusion center response and readiness, banking**

> *"Immersive's activities and scenarios are crafted with more depth realism than [those we've used in the past]."*
>
> **VP of program management and strategic projects, managed services**

Improved Organizational Security Posture					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
E1	Cumulative cost of breaches for the composite	Forrester research	$4,427,000	$4,427,000	$4,427,000
E2	Likelihood of experiencing one or more breaches for the composite	Forrester research	68%	68%	68%
E3	Percentage of breaches originating from external attacks targeting organizations, external attacks targeting remote environments, internal incidents, attacks, or incidents involving the external ecosystem	Forrester research	90%	90%	90%
E4	Percentage of those attacks addressable with Immersive One	Interviews	90%	90%	90%
E5	Annual risk exposure addressable with Immersive One	D1*D2*D3*D4	$2,438,392	$2,438,392	$2,438,392
E6	Reduced risk of exposure to breach costs from addressable attacks with Immersive One	Interviews	5%	5%	5%
Et	Improved organizational security posture	E5*E6	$121,920	$121,920	$121,920
	Risk adjustment	↓15%			
Etr	Improved organizational security posture (risk-adjusted)		$103,632	$103,632	$103,632
	Three-year total: $310,895			**Three-year present value: $257,717**	

Unquantified Benefits

Interviewees mentioned the following additional benefits that their organizations experienced but were not able to quantify:

- **Higher cybersecurity awareness within the organization.** Inherent with a higher adoption of cyber resilience labs and exercises across the organizations' different roles was a higher awareness of security preparedness and response across entire organizations. By leveraging Immersive One, interviewees noted that security culture at their organizations was more top of mind. Beyond the annualized risk exposure quantified for this report, this improvement to security posture may help an organization avoid major security breaches that may result in fines or reputational damage. Several interviewees noted that regional cybersecurity teams within their organizations compete with other teams across the globe in friendly competition on Immersive, illustrating the broader security culture benefit supported by Immersive's gamification.
- **Employee experience and upskilling.** Beyond the employee retention benefits as quantified for this report (benefits A and B), interviewees explained that Immersive One engages cybersecurity personnel in a way that previous options did not, driving higher engagement, skills development, and ultimately higher job satisfaction and upskilling for promotions.
- **Security framework and compliance standard alignment.** Several interviewees explained that Immersive One allowed their organizations to map skills and capabilities to security frameworks and meet compliance standards. The interviewee at the managed services firm noted: "Immersive [was selected over competitors] due to the completeness of the lab sets and the ability to really map our team's capabilities back to the MITRE [ATT&CK] framework. Being able to see these competencies at an individual level and at a team level gave us consistency in how we thought about our cybersecurity team skills." The

interviewee at the European insurance organization added: "We were going after ISO 27001 as an organization, which involves talking to a lot of different people in front of auditors. Our network that's developed and grown through Immersive One massively contributed to making that process a lot smoother than it could have been."

- **Hiring and onboarding skills assessments.** Interviewees explained that Immersive One's labs and exercises are now (or soon will be) used as part of their organizations' hiring processes, ensuring that candidates are the most qualified for the positions for which they're being recruited, potentially reducing onboarding costs, and further improving attrition. The interviewee at the managed services firm noted that cybersecurity onboarding times have decreased by 25% from 100 days to 75 days on average, while the telecommunications organization is using Immersive Talent to ensure that candidates have the skills they need for the roles they're being hired for.
- **Shorter SDLCs.** By leveraging Immersive One across their organizations' developer bases, some interviewees noted that developers spend less time remediating vulnerabilities further in the SDLC, not only saving developer time (as quantified in benefit C) but also accelerating software delivery to internal clients or customers.

25%+ improvement

Average cybersecurity onboarding time

> *"Immersive [One] gives us a depth of knowledge that we can quantify across different views like the MITRE ATT&CK framework. We can actually quantify the breadth and depth of coverage we have in the organization and zoom in on specific teams as needed. The ability to summarize and quantify this knowledge is quite impressive."*
>
> **Cybersecurity education and awareness lead, banking**

> *"Immersive [One] delivers real-world scenarios that actually keep our team members engaged. It's not just 'watch this video' or 'click these buttons,' but a hands-on approach that's yielded some of the best feedback we've gotten from our team members."*
>
> **VP of program management and strategic projects, managed services**

Flexibility

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

- **Expanding Immersive One across other roles within the organization.** Although several organizations leveraged Immersive One across all roles, some interviewees explained that there were still more roles to cover with Immersive One, potentially driving additional cost savings and security posture improvements.
- **Staying current on the evolving threat landscape.** Interviewees explained that when it identifies new or emerging threats or vulnerabilities, Immersive One is quick to have a lab or exercise aimed at improving preparedness or response. Over time, this may result in avoiding security breach-related costs for organizations as they continue to leverage Immersive.

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Total Economic Impact Approach).

> *"Threats are always evolving and Immersive is meeting our needs to stay on top of those threats. When it's through the labs or through the simulations, we've always got up-to-date and relevant content. Staying current is a critical concern for our clients and our regulators and Immersive continues to help us address these concerns."*
>
> **Global lead, cybersecurity fusion center response and readiness, banking**

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	Immersive subscription fees	$0	$250,000	$250,000	$250,000	$750,000	$621,713
Gtr	Immersive internal program management costs	$11,000	$16,500	$16,500	$16,500	$60,500	$52,033
	Total costs (risk-adjusted)	$11,000	$266,500	$266,500	$266,500	$810,500	$673,746

Immersive Subscription Fees

Interviewees paid for their Immersive products based on several factors, including number of employees exercised and their roles; frequency and access to labs and exercises; and the specific types of labs, exercises, and simulations. Pricing for the composite organization has been conservatively estimated for the configuration below. Pricing may vary. Contact Immersive for additional details or pricing specific to your organization.

Modeling and assumptions. For the composite organization, Forrester makes the following assumptions:

- There is a $250,000 annual investment with Immersive for 4,200 users (200 cybersecurity personnel, 1,000 developers, and 3,000 wider workforce members, including the executive team). For these roles, the investment includes:
  - Hands-on labs: Each user group receives unlimited access to labs relative to their roles.
  - Cyber range exercises: All cybersecurity personnel have access to a cyber range exercise once per quarter to be completed in teams.
  - Crisis simulations: Each user has access to crisis simulations (monthly) to test nontechnical decision-making against crisis response playbooks.
  - Workforce exercises: The wider workforce has unlimited access to micro exercises to gauge the wider risk profile of the business, with targeted labs assigned based on performance to address improvement areas.

Risks. This cost will vary among organizations based on:

- The number of employees (and their roles) licensed on Immersive One.
- The specific crisis simulations, drills, or exercises included.
- The access to and/or frequency of these exercises.

Results. Though variances may exist, Forrester did not risk adjust this cost since it is a direct estimate for the composite organization, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $622,000.

Immersive Subscription Fees						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
F1	Immersive subscription fees	Immersive		$250,000	$250,000	$250,000
Ft	Immersive subscription fees	E1	$0	$250,000	$250,000	$250,000
	Risk adjustment	0%				
Ftr	Immersive subscription fees (risk-adjusted)		$0	$250,000	$250,000	$250,000
	Three-year total: $750,000			**Three-year present value: $621,713**		

Immersive Internal Program Management Costs

Interviewees collectively described the level of internal personnel effort required to maintain the Immersive relationship and ensure users maximized their access. Common tasks required for internal resources included managing user and team access, interfacing with Immersive' s support team, and planning simulations for cybersecurity teams.

Modeling and assumptions. For the composite organization, Forrester makes the following assumptions:

- One FTE dedicates 10% of their working hours to maintaining the Immersive One platform and relationship on tasks such as managing user access, planning Immersive One exercises, and working with Immersive's account management and support team.
- The average fully burdened annual salary for an FTE managing the Immersive relationship is $150,000.

Risks. This cost may vary among organizations based on:

- The knowledge and/or capacity of internal resources managing the Immersive relationship.
- The scope of an organization's Immersive-licensed user base related to the level of effort required to support access, exercises, and related tasks.
- Any additional Immersive-related work that requires additional FTE effort (e.g., planning for and supporting security framework alignment).

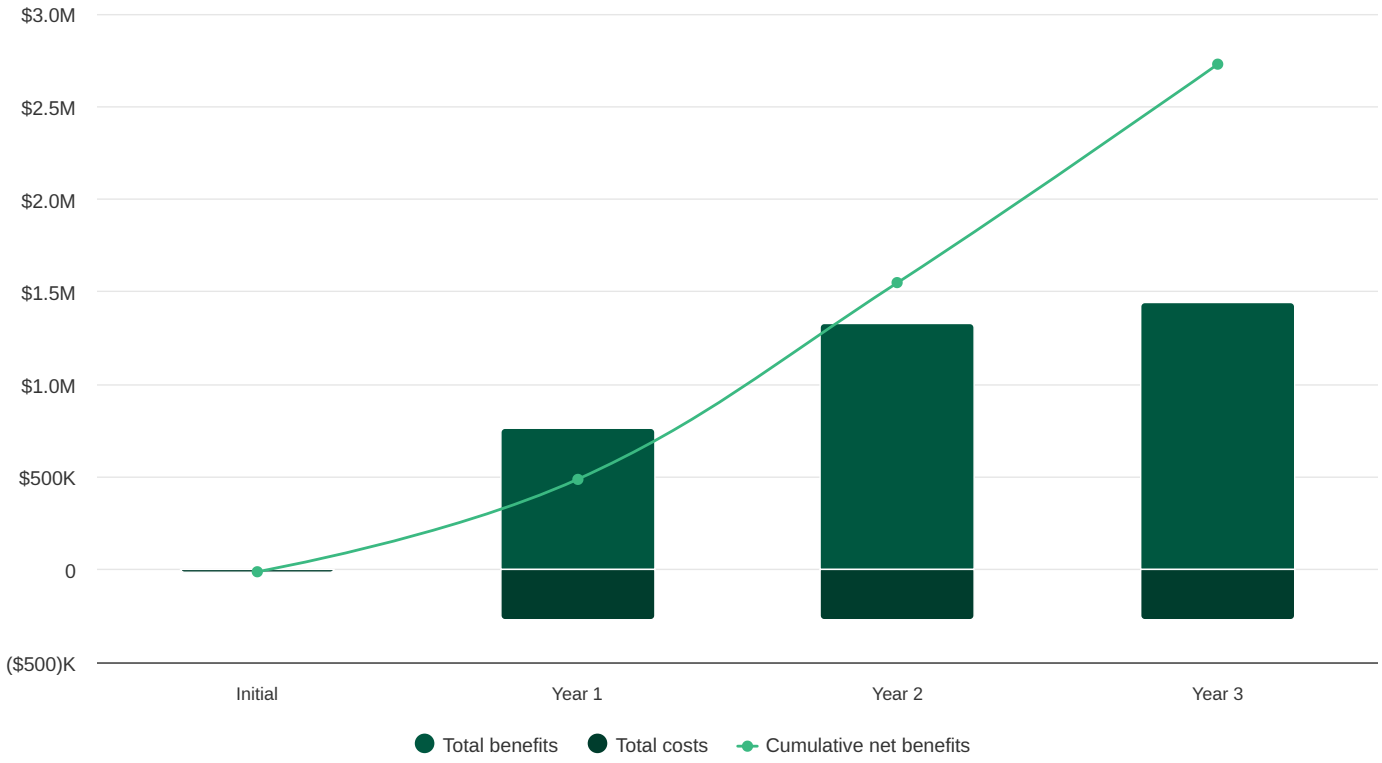
Results. To account for these variances, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $52,000.

Immersive Internal Program Management Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
G1	Initial Immersive onboarding costs	Composite	$10,000			
G2	FTEs responsible for Immersive on an ongoing basis	Composite		1	1	1
G3	Fully burdened annual salary for an FTE managing the Immersive relationship	Composite		$150,000	$150,000	$150,000
G4	Percentage of time dedicated to Immersive-related tasks	Interviews		10%	10%	10%
Gt	Immersive internal program management costs	G1+(G2*G3*G4)	$10,000	$15,000	$15,000	$15,000
	Risk adjustment	↑10%				
Gtr	Immersive internal program management costs (risk-adjusted)		$11,000	$16,500	$16,500	$16,500
	Three-year total: $60,500			**Three-year present value: $52,033**		

Financial Summary

Consolidated Three-Year, Risk-Adjusted Metrics

Cash Flow Chart (Risk-Adjusted)



Cash Flow Analysis (Risk-Adjusted)						
	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($11,000)	($266,500)	($266,500)	($266,500)	($810,500)	($673,746)
Total benefits	$0	$765,067	$1,328,817	$1,445,692	$3,539,575	$2,879,880
Net benefits	($11,000)	$498,567	$1,062,317	$1,179,192	$2,729,075	$2,206,134
ROI						327%
Payback						<6 months

Please Note

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.

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 calculations are calculated for each total cost and benefit estimate. NPV calculations in 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.

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 Immersive One.

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 Immersive One can have on an organization.

Due Diligence

Interviewed Immersive stakeholders and Forrester analysts to gather data relative to Immer.

Interviews

Interviewed six decision-makers at organizations using Immersive One to obtain data about 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 interviewees.

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.

Glossary

Total Economic Impact Approach

Benefits

Benefits represent the value the solution delivers to the business. The TEI methodology places equal weight on the measure of benefits and costs, allowing for a full examination of the solution's effect on the entire organization.

Costs

Costs comprise all expenses necessary to deliver the proposed value, or benefits, of the solution. The methodology captures implementation and ongoing costs associated with the solution.

Flexibility

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

Risks

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."

Financial Terminology

Present value (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PVs 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

The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Appendixes

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 solution providers in communicating their value proposition to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of business and technology initiatives to both senior management and other key stakeholders.

APPENDIX B

Endnotes

[1] Source: The Cybersecurity Skills And Training Platforms Landscape, Q4 2025, Forrester Research, Inc., October 8, 2025.

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

[3] Source: Forrester's Security Survey, 2025. This study analyzes broad patterns among security decision-makers across multiple areas related to an organization's cybersecurity practices. While this study primarily provides insight into the priorities, investments, and customer journeys of decision-makers, it also includes questions about general priorities as well as standard demographic and firmographic questions. Forrester annually assesses cybersecurity metrics through interviews, surveys, and expertise in the field.

[4] Ibid.

Disclosures

Readers should be aware of the following:

This study is commissioned by Immersive 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 study to determine the appropriateness of an investment with Immersive. For any interactive functionality, the intent is for the questions to solicit inputs specific to a prospect's business. Forrester believes that this analysis is representative of what companies may achieve with Immersive based on the inputs provided and any assumptions made. Forrester does not endorse Immersive or its offerings. Although great care has been taken to ensure the accuracy and completeness of this model, Immersive and Forrester Research are unable to accept any legal responsibility for any actions taken on the basis of the information contained herein. The interactive tool is provided 'AS IS,' and Forrester and Immersive make no warranties of any kind.

Immersive 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.

Immersive provided the customer names for the interviews but did not participate in the interviews.

Consulting Team:
Richard Cavallaro

PUBLISHED
January 2026