FORRESTER®

The Total Economic Impact™ Of SimSpace

Cost Savings And Business Benefits Enabled By SimSpace

A FORRESTER TOTAL ECONOMIC IMPACT STUDY
COMMISSIONED BY SIMSPACE, MARCH 2025

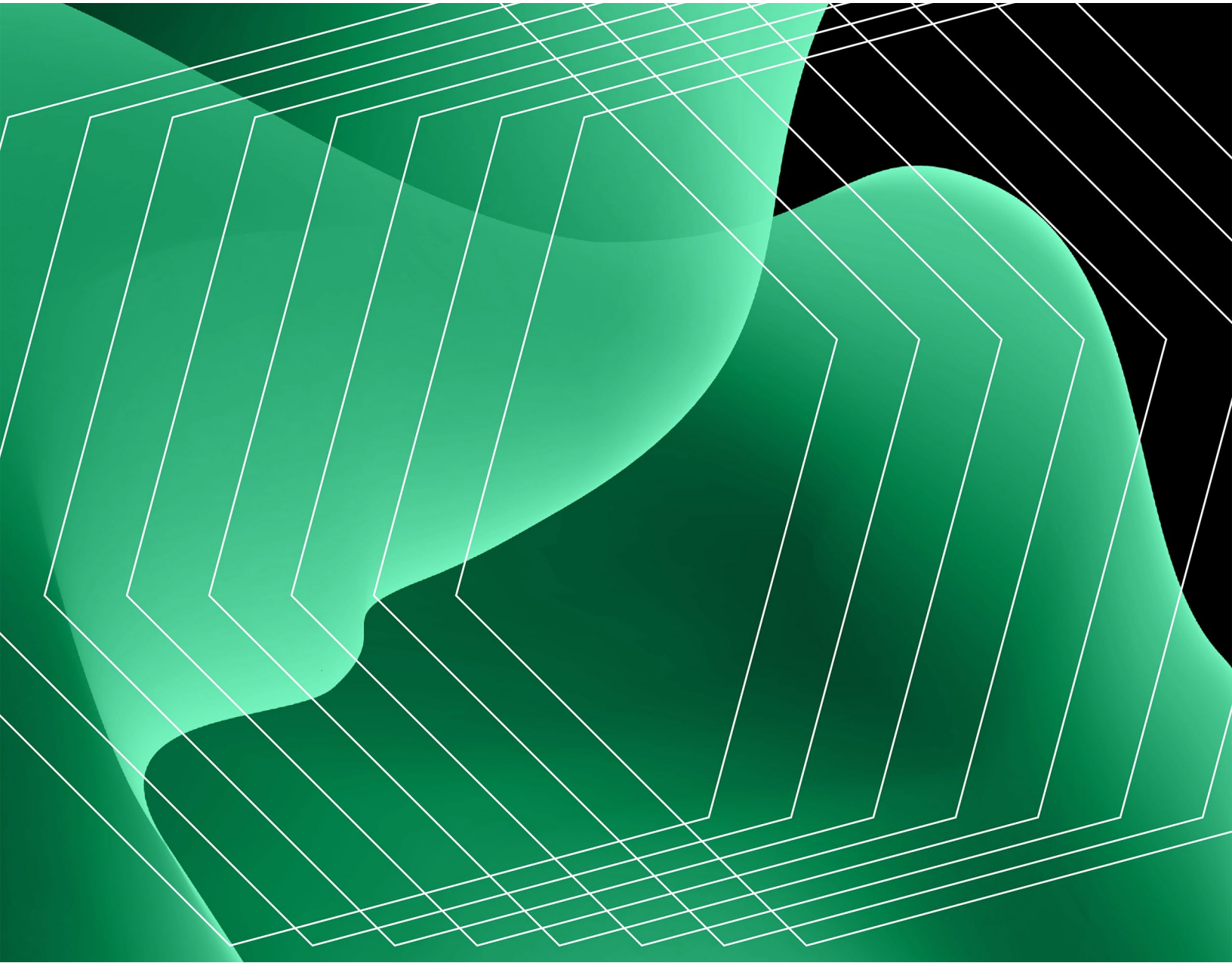


Table Of Contents

Consulting Team:

Jonathan Whaling

ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute their specific priorities using a unique engagement model that ensures lasting impact. For more information, visit forrester.com/consulting.

© Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies.

Executive Summary

Cyber range solutions prepare cybersecurity teams for cyberattacks by taking them through simulated, realistic exercises and testing scenarios. Large organizations in vulnerable industries are turning to cyber range solutions to supplement or replace other forms of security training as well as to engage in security testing. These solutions enable security staff to save time in detecting and remediating cyberthreats, as well as assist security teams in testing new tools and developing detections and alerts for new threats and vulnerabilities.

SimSpace provides cyber ranges that enable realistic simulation exercises and testing against cyberattacks, along with guidance and evaluation services. Large organizations can turn to SimSpace to run these cyber drills to train, test, and prepare their security teams to quickly and efficiently defend against evolving threats. SimSpace also provides other cyber range testing and training use cases for testing tools, tactics, and policies, as well as course- and lab-based training for security staff.

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

Return on investment (ROI)
127%

Net present value (NPV)
$2.2M

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five decision-makers with experience using SimSpace. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is a global financial services organization with 20,000 employees and revenue of $25 billion per year.

Interviewees said that prior to using SimSpace, their organizations lacked a comprehensive way to put their cybersecurity teams through real-world training scenarios. They also lacked

controlled environments for testing new security tools and tactics. The interviewees' organizations had implemented a full stack of monitoring and detection tools but had not conducted comprehensive testing with their entire teams. Previously, they conducted mainly classroom and on-the-job training with security operations staff and were looking to raise their game with simulated, full-scope attack scenarios.

After the investment in SimSpace, the interviewees stated their teams were far better prepared to defend against cyberattacks and generally exhibited higher engagement and job satisfaction. Beyond the cyber drills, interviewees' organizations that used a SimSpace cyber range in a lab environment realized efficiencies and other savings in managing their security tools and tactics.

KEY FINDINGS

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

- **Reduced mean time to remediate security breaches.** After one or more cyber drills, the composite organization improves its mean time to remediate (MTTR) a security breach by 40% in Year 1. This percentage grows to 50% in Year 3. The composite organization saves $2.9 million in engineer productivity over three years.
- **Reduced the exposure to security breaches due to faster detection and remediation times.** After one or more cyber drills in Year 1, the composite organization reduces its mean time to detect (MTTD) a breach by 20% and its mean time to remediate a breach by 40%. The composite organization saves $379,000 in potential exposure over three years.
- **Reduced annual cyber security training expenses with a focus on team-based training exercises.** The composite organization replaces spending on individual and classroom-based training programs with team-based cyber drill events, which occur twice annually. The savings amount to $396,000 over three years.
- **Accelerated time to deploy new security tools by four months due to testing in a cyber range lab environment.** The composite organization rolls out new security tools four months faster due to testing in a lab environment rather than production. This translates to savings of $136,000 in potential exposure over three years.

- **Saved 300 hours per year of cyber engineers' time by developing threat detections in the lab environment.** By using the lab environment to develop detections and alerts to new threats emerging in the market, the composite saves engineers 300 hours of time annually, which translates to $46,000 over three years.

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

- **Range training exercises create high levels of satisfaction and confidence among teams.** Compared to individual or classroom training, SimSpace training exercises are more engaging and collaborative, leading to higher levels of satisfaction and team morale at the composite organization.
- **The existence of a cyber range environment helps attract and retain highly qualified hires.** With SimSpace, the composite organization can both attract more qualified job applicants and retain high-performing cyber professionals.
- **Regular training exercises enable testing and refinement of incident response playbooks.** A common input and output of training exercises are incident response playbooks. The composite stress tests these playbooks under operational conditions during cyber drills and then updates them after the drills to improve future processes.
- **Output from training exercises saves time and provides critical evidence for regulators and auditors.** SimSpace after-action reports provide critical performance metrics as output from the cyber drills both for enhancing response processes and presenting results to auditors.
- **Detection engineering teams build and test detection rules and alerts before porting them over to production.** A common use of the SimSpace lab environment for the composite organization is testing and validating detection rules and alerts before rolling them out in production.

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

- **Annual subscription fees of $1.3 million over three years.** SimSpace software-as-a-service (SaaS) fees are based on the use cases the customer deploys, concurrent users, and virtual machines (VMs). For the composite organization, this fee is $525,000 per year for up to 60 concurrent users and 300 VMs.

- **Internal maintenance and planning costs of $161,000 over three years.** This consists of fully burdened annual salaries for two engineers at 20% time.
- **Annual travel costs of $246,000 over three years.** As an optional expense, this consists of travel costs for 15% of security staff for two events each year.

The representative interviews and financial analysis found that the composite organization experiences benefits of $3.9 million over three years versus costs of $1.7 million, adding up to a net present value (NPV) of $2.2 million and an ROI of 127%.

> "SimSpace allows our cyberdefenders to see real-world attacks happening on our network and respond to them. It's the closest thing to a real-world environment."
>
> **DIRECTOR OF INFORMATION SECURITY, FINANCIAL SERVICES**

> "I would start [by looking] at cost avoidance in training. It costs $3,000 per person [for an external training] course. We can get our biggest bang for our buck here. Once you add in team-oriented metrics like knowing how quickly it takes us to respond to a specific threat — you don't get that anywhere else."
>
> **VP, CYBERSECURITY ENGINEERING, MORTGAGE FINANCING**

Return on investment (ROI)

127%

Benefits PV

$3.9M

Net present value (NPV)

$2.2M

Payback

<6 months

Benefits (Three-Year)

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 SimSpace cybersecurity skills and training platforms.

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 SimSpace cybersecurity skills and training platforms can have on an organization.

Due Diligence
Interviewed SimSpace stakeholders and Forrester analysts to gather data relative to its use in practice.

Interviews
Interviewed five people at organizations using SimSpace 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.

DISCLOSURES
Readers should be aware of the following:

This study is commissioned by SimSpace 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 in SimSpace.

SimSpace 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.

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

The SimSpace Customer Journey

Drivers leading to the investment

Interviews				
Role	**Industry**	**Region**	**Annual Revenue**	**Number Of Employees**
Head of vulnerability and patch management	Financial services	North America	$82 billion	225,000
VP, cybersecurity engineering	Mortgage financing	North America	$29 billion	8,000
Director of information security	Insurance and investment	North America	$46 billion	25,000
VP, incident response leader	Credit card processing	North America	$24 billion	20,000
Professor	Education	North America	$800 million (est.)	8,500

KEY CHALLENGES

Interviewees' organizations faced challenges in creating realistic testing environments, evaluating the efficacy of new tools, and ensuring their teams were adequately prepared for cyberthreats. Existing training and testing methods presented limitations for cybersecurity teams. With an ongoing focus on preparedness for cybersecurity threats, some of the interviewees noted their organizations hired new executives to lead these efforts.

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

- **Existing cybersecurity training methods that focused on individuals and were limited in their effectiveness.** Interviewees' organizations relied on training methods that were centered on individual team members, such as external training classes, online courses, on-the-job learnings, and other ad hoc methods. Some interviewees noted their organizations employed tabletop exercises, which lacked testing realistic attack scenarios. Any realistic training or testing scenario conducted in the production environment would risk significant operational impacts.

- **Risks associated with rolling out new security tools and making other changes in production environments.** Interviewees reported that testing new security tools and threat actor tactics, techniques, and procedures (TTPs) in the production environment required opening admin-level access, which posed significant risks.
- **Disruption of in-person testing and training activities due to the COVID-19 pandemic.** The professor at an education organization said their organization conducted its classes solely in person, so it had to quickly find a platform to pivot to online at the beginning of the pandemic. Other interviewees also noted that the pandemic prevented the tabletop exercises they previously employed.

SOLUTION REQUIREMENTS

The interviewees' organizations searched for a solution that could:

- Conduct live fire cyber range exercises to simulate real-world scenarios. Going into an exercise, the interviewees noted their organizations wanted to define each scenario around an advanced persistent threat (APT) and then use the exercises to demonstrate preparedness to regulators and auditors.
- Provide realistic training scenarios with a focus on team-based exercises to improve the skills, collaboration, and response capabilities of the security team as a whole.
- Enable after-action reports to identify areas for improvement and process changes that could feed into incident response plans and playbooks.
- Reduce time to value in security engineering by setting up a testing environment (lab) that closely matched production.

Most of the interviewees said their organizations did not go through a formal evaluation and selection process for SimSpace. Instead, CISOs at their organizations had familiarity with SimSpace from previous employers and knew about its long-standing use in the United States Department of Defense. Interviewees noted other organization-specific reasons for choosing SimSpace, including the following:

- Three interviewees said their organizations desired the ability to conduct large-scale, live-fire cyber range exercises and realistic simulations on a semiannual or more frequent basis. These exercises needed to provide an ability to simulate real-world scenarios and react to them as a team.

- The VP, incident response leader at the credit card processing organization reported that their organization was looking for a testing (lab) environment to facilitate faster deployment of new security tools and updates, especially during production change freeze windows. By becoming familiar with new tools and testing new threat detections in the lab, engineers could streamline the deployment process once a production freeze was lifted.
- The professor at the education organization noted their organization was looking to expand its cybersecurity training program from an in-person lab to an online environment. They wanted to reduce instructor time spent on student setup and maintenance activities, allowing them to focus more on course development and student assessment.

> "We wanted to find a way to understand a few different things. [First], how good do we know our tools really are against a real adversary? How good are our folks in any situation where they are required to battle an adversary? [And finally], how do we find a solution to measure that? We looked and looked, and we came across SimSpace."
>
> **VP, CYBERSECURITY ENGINEERING, MORTGAGE FINANCING**

> "What SimSpace is giving you is [the ability to use] your own tools. The tools that you want to use, the tools that you fight with every single day, you can have in the lab."
>
> **VP, INCIDENT RESPONSE LEADER, CREDIT CARD PROCESSING**

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 is a global, multibillion-dollar consumer and business banking organization that provides a range of financial services products, including transaction accounts, savings accounts, and a variety of credit products. The composite organization is based in the US with 20,000 employees worldwide. It has 150 employees on its security staff, which is based on three continents. Its annual security budget is $35 million, which includes software, staff, and outside services.

Deployment characteristics. There is no deployment period for SimSpace as it is a cloud-based service. The composite spends about two to three weeks preparing for full-scale cyber drills twice a year. Smaller, more focused drills require a week or less of prep time. These activities included the following:

- Establishing clear objectives for the drill, such as testing specific TTPs or validating incident response plans
- Creating realistic scenarios based on actual threats or APTs relevant to the organization
- Configuring the cyber range, covering all production security tools
- Obtaining necessary licenses for tools and ensuring all participants have appropriate access
- Identifying key teams, including incident response, red team, blue team, and any other relevant stakeholders
- Establishing detailed schedules, shift handovers, and key milestones

The composite also uses SimSpace in a lab environment, which does not have event preparation activities per se. Rather, the lab is used on an ongoing basis by one or a few engineers at a time. The lab is set up to mimic the production environment, so individual security engineers use it as part of their processes to test new TTPs or perform proofs of concept (POCs) on new security tools or modules.

Key Assumptions

$25 billion in annual revenue

20,000 employees

Annual security budget of $35 million

Total security staff of 150

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	Incremental productivity improvement per cybersecurity engineer	$1,056,580	$1,188,652	$1,320,725	$3,565,957	$2,935,164
Btr	Reduced exposure to breaches due to faster detection and remediation of incidents	$131,704	$153,712	$175,719	$461,135	$378,786
Ctr	Reduced annual training costs for cybersecurity teams	$159,375	$159,375	$159,375	$478,125	$396,342
Dtr	Reduced exposure of a likely security breach due to accelerated tool deployment	$54,782	$54,782	$54,782	$164,346	$136,235
Etr	Time savings from developing threat detections in lab environment	$18,360	$18,360	$18,360	$55,080	$45,659
	Total benefits (risk-adjusted)	$1,420,801	$1,574,881	$1,728,961	$4,724,643	$3,892,186

INCREMENTAL PRODUCTIVITY IMPROVEMENT PER CYBERSECURITY ENGINEER

Evidence and data. Interviewees noted cyber drills offered realistic simulations of various cyberthreats and cyberattacks. This allowed security employees to experience and understand the complexities of different attack vectors, learn how to detect and respond to them, and develop effective mitigation strategies.

- The interviewees' organizations reported noticeable reductions in the time it took to detect and remediate incidents due to the practical experience and insights gained from the drills. Specifically, interviewees reported improvements of 30% to 60% in MTTR after one or more cyber drill events.

- The drills allowed the interviewees' organizations to test their incident response plans. After the events, they refined those plans, which in turn led to more efficient and effective remediation processes.
- Interviewees noted a direct by-product of the cyber drills exercises was enhanced teamwork in responding to threats. The VP of cybersecurity engineering noted their mortgage financing organization realized rapid efficiency gains in solving problems. The exercises helped break down barriers that existed between security teams. The interviewee explained: "I'm a big fan of crowdsourcing. If I can take three people and assign them together to solve a problem, like finding a threat, it can be more effective. [With SimSpace], I can create a channel to allow that cross-pollination to happen."

Modeling and assumptions. Forrester assumes the following about the composite organization:

- The composite organization has 150 cybersecurity FTEs, of which 38% are engaged in incident response activities. These roles include incident responders, detection engineers, and security information and event management (SIEM) engineers. It is assumed that these roles devote 75% of their time to a single threat.[2]
- The composite experiences an average number of 2.6 data breaches each year.[3]
- The mean time to respond to a breach for the composite is 51.3 days.[4]
- The fully burdened annual salary for a cybersecurity professional is $136,282. This equates to a daily rate of $545.
- After SimSpace cyber drills, the improvement in MTTR is 40% in Year 1. Incremental improvements in Years 2 and 3 decline from Year 1 but increase cumulatively as compared to before SimSpace.

Risks. The expected financial impact of this benefit is subject to risks and variation based on the following factors:

- The frequency of threats requiring investigation and remediation, which depend upon the efficacy of various security tools in production.
- MTTR baseline and improvements, which depend on the sophistication of detection and response engineering teams and tools at an organization.
- Salaries and burden rates.

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 $2.9 million.

40%

Year 1 improvement in MTTR after SimSpace drills

"The live fire range exercises have significantly improved our team's ability to detect and respond to incidents. We've seen a noticeable reduction in remediation times as a result."

DIRECTOR OF INFORMATION SECURITY, INSURANCE AND INVESTMENT

Incremental Productivity Improvement Per Cybersecurity Engineer					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Cybersecurity FTEs	Composite	150	150	150
A2	Fully burdened daily rate for a cybersecurity engineer	TEI standard	$545	$545	$545
A3	Percentage of cybersecurity team involved in incident response	Forrester research	38%	38%	38%
A4	Percentage of time devoted to incident response	TEI assumption	75%	75%	75%
A5	Mean number of data breaches per year	Forrester research	2.6	2.6	2.6
A6	Average MTTR before SimSpace (days)	Forrester research	51.3	51.3	51.3
A7	Percentage improvement in MTTR	Interviews	40%	45%	50%
At	Incremental productivity improvement per cybersecurity engineer	A1*A2*A3*A4*A5*A6*A7	$1,243,035	$1,398,414	$1,553,794
	Risk adjustment	↓15%			
Atr	Incremental productivity improvement per cybersecurity engineer (risk-adjusted)		$1,056,580	$1,188,652	$1,320,725
	Three-year total: $3,565,957			**Three-year present value: $2,935,164**	

REDUCED EXPOSURE TO BREACHES DUE TO FASTER DETECTION AND REMEDIATION OF INCIDENTS

Evidence and data. The risk and cost of a security breach was top-of-mind for all the interviewees' organizations. Interviewees cited the financial impact of a breach, damage to their organizations' reputations, and operational disruptions as potential risks and losses. Interviewees were concerned about business continuity, loss of reputation and trust, and direct costs associated with restoring systems and data.

- The hands-on experience gained from SimSpace drills led interviewees' organizations to the quicker detection and remediation of incidents, minimizing the impact of any breaches. In addition to remediation improvements mentioned in the last benefit, organizations reduced their MTTD by 20% to 25%. MTTR improvements after SimSpace cyber drills varied from 30% to 60%.
- Some interviewees noted SimSpace provided their organizations with validation and fine-tuning of detection rules, which reduced false positives and ensured accurate threat detection. The head of vulnerability and patch management said their organization

reduced the number of threats by several hundred a month by developing new rules and refining existing ones in the cyber range.

Modeling and assumptions. Forrester assumes the following about the composite organization:

- The likelihood of experiencing one or more security breaches in a year is 54%.[5]
- The mean cumulative cost of a security breach is $3.4 million per year, or $9,274 per day.[6]
- The mean time to detect a breach is 52.1 days and the mean time to respond is 51.3 days.[7]
- After SimSpace cyber drills, the improvement in MTTD is 20% in Year 1. Incremental improvements in Years 2 and 3 decline from Year 1 but increase cumulatively compared to before SimSpace.
- After SimSpace cyber drills, the improvement in MTTR is 40% in Year 1. Incremental improvements in Years 2 and 3 decline from Year 1 but increase cumulatively compared to before SimSpace.

Risks. The expected financial impact of this benefit is subject to risks and variation based on the following factors:

- MTTD and MTTR baseline and improvements, which depend on the sophistication of detection and response engineering teams and tools at an organization.
- The frequency of threats requiring investigation and remediation, which depend upon the efficacy of various security tools in production.
- The estimated cost of a security breach, which depend upon its scope and depth of data exposed, along with the extent of employees involved in recovery.

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 $379,000.

20%

Year 1 improvement in MTTD after SimSpace drills

"The investment in SimSpace is well worth it because the repercussions of a data breach would be many times that investment."

DIRECTOR OF INFORMATION SECURITY, INSURANCE AND INVESTMENT

Reduced Exposure To Breaches Due To Faster Detection And Remediation Of Incidents					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Likelihood of experiencing one or more breaches	Forrester research	54%	54%	54%
B2	Mean cumulative cost of breaches (per day)	Forrester research	$9,274	$9,274	$9,274
B3	Average MTTD before SimSpace (days)	Forrester research	52.1	52.1	52.1
B4	Percentage improvement in MTTD	Interviews	20%	25%	30%
B5	**Subtotal: Reduced exposure due to faster detection**	**B1*B2*B3*B4**	**$52,183**	**$65,229**	**$78,274**
B6	Average MTTR before SimSpace (days)	Forrester research	51.3	51.3	51.3
B7	Percentage improvement in MTTR	Interviews	40%	45%	50%
B8	**Subtotal: Reduced exposure due to faster remediation**	**B1*B2*B6*B7**	**$102,763**	**$115,609**	**$128,454**
Bt	Reduced exposure to breaches due to faster detection and remediation of incidents	B5+B8	$154,946	$180,838	$206,728
	Risk adjustment	↓15%			
Btr	Reduced exposure to breaches due to faster detection and remediation of incidents (risk-adjusted)		$131,704	$153,712	$175,719
	Three-year total: $461,135			**Three-year present value: $378,786**	

REDUCED ANNUAL TRAINING COSTS FOR CYBERSECURITY TEAMS

Evidence and data. While not all interviewees said their organizations claimed a reduction in training expenses, those that did reported significant savings after switching to SimSpace as the primary training provider.

- Interviewees reported that realistic training scenarios SimSpace provided were more engaging and enjoyable for employees compared to traditional methods, leading to higher satisfaction.
- Even in a lab environment, interviewees said the hands-on range experience contributed to organic training and skill development for the security teams. This also reduced the need for expensive external training courses.

- Interviewees also reported that another benefit of SimSpace was that everyone on the security team trains together, yielding more effective and cohesive results.

Modeling and assumptions. Forrester assumes the following about the composite organization:

- The number of security FTEs in the composite organization is 150.
- Average annual costs for training per employee are $2,500.
- The reduction in training expenses after investing in SimSpace is 50%.

Risks. The expected financial impact of this benefit is subject to risks and variation based on the training budgets, which will vary based on several organizational factors.

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 $396,000.

> "Having a cloud-based range allows global teams to train together, which saves costs."
>
> DIRECTOR OF INFORMATION SECURITY, INSURANCE AND INVESTMENT

Reduced Annual Training Costs For Cybersecurity Teams					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Cybersecurity FTEs	Composite	150	150	150
C2	Annual training costs per FTE	Interviews	$2,500	$2,500	$2,500
C3	Reduction in training costs after SimSpace	Interviews	50%	50%	50%
Ct	Reduced annual training costs for cybersecurity teams	C1*C2*C3	$187,500	$187,500	$187,500
	Risk adjustment	↓15%			
Ctr	Reduced annual training costs for cybersecurity teams (risk-adjusted)		$159,375	$159,375	$159,375
	Three-year total: $478,125			**Three-year present value: $396,342**	

REDUCED EXPOSURE OF A LIKELY SECURITY BREACH DUE TO ACCELERATED TOOL DEPLOYMENT

Evidence and data. According to interviewees, integrating new tools into their organizations' existing security ecosystem often required significant effort and expertise. The interviewees' organizations needed to verify that new tools would not disrupt current operations or conflict with other security solutions. This included configuring tools to work seamlessly with other security measures and ensuring they could effectively communicate and share data. There were concerns about the potential impact of new tools on system performance. To address this, the interviewees' organizations used the SimSpace cyber range in a variety of ways:

- The head of vulnerability and patch management noted their organization fine-tuned tool configurations and detection rules, ensuring the tools were optimized for their specific infrastructure and threat landscape.
- The VP, incident response leader in credit card processing said their organization used SimSpace's lab environment to allow engineers to get familiar with new tools. This reduced the learning curve and ensured that staff were proficient in using the tools before they were deployed in production.
- The VP, incident response leader at the credit card processing organization also said their credit card processing organization used the cyber range for testing new products to help them make informed decisions on tools to buy and deploy. This interviewee explained: "Here, I can put [the new tools] in the range. I can throw actual ransomware

at it and measure [one tool] versus [another]. I can run scenarios against each of these products and have real results on how good something is."

Modeling and assumptions. Forrester assumes the following about the composite organization:

- The likelihood of experiencing one or more security breaches in a year is 54%.[8]
- The mean cumulative cost of a security breach is $3.4 million per year.[9]
- The reduction in risk exposure from a new security tool is 10%. This can vary but was evidenced in more than one organization in the study.
- The acceleration in production rollout time is estimated to be four months, or one-third of a year.
- Time savings from testing tools in a lab environment rather than in production is not factored into the model but can be assumed to enhance this benefit.

Risks. The expected financial impact of this benefit is subject to risks and variation based on the following factors:

- The frequency of threats requiring investigation and remediation, which will depend upon the efficacy of various security tools in production.
- The estimated cost of a security breach, which will depend upon its scope and depth of data exposed, along with the extent of employees involved in recovery.

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 $136,000.

> **4 months**
>
> Acceleration in new security tool deployment

> "We reduced what was a six- to eight-month deployment window down to two months."
>
> VP, INCIDENT RESPONSE LEADER, CREDIT CARD PROCESSING

Reduced Exposure Of A Likely Security Breach Due To Accelerated Tool Deployment					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	Likelihood of experiencing one or more breaches	Forrester research	54%	54%	54%
D2	Mean cumulative cost of breaches	Forrester research	$3,385,000	$3,385,000	$3,385,000
D3	Reduced risk of a breach per new tool	Interviews	10%	10%	10%
D4	Acceleration in production deployment time	Interviews	33.3%	33.3%	33.3%
Dt	Reduced exposure of a likely security breach due to accelerated tool deployment	D1*D2*D3*D4	$60,869	$60,869	$60,869
	Risk adjustment	↓10%			
Dtr	Reduced exposure of a likely security breach due to accelerated tool deployment (risk-adjusted)		$54,782	$54,782	$54,782
	Three-year total: $164,346			**Three-year present value: $136,235**	

TIME SAVINGS FROM DEVELOPING THREAT DETECTIONS IN LAB ENVIRONMENT

Evidence and data. The VP, incident response leader at the credit card processing organization described a use case specific to the lab environment was the development of threat detections and alerts in the lab rather than in a production environment. This interviewee said their organization previously built detections in production, which meant security operation center (SOC) analysts had to respond to false positives and then sort those out with the detection engineers.

- Interviewees said that in the past, detection engineers developed 40 to 60 new detections each month based on new tactics, techniques, and procedures (TTPs).

- They also said each detection and alert required 30 minutes of time on average between security operations and detection engineering to rectify false positives and adjust alerts.
- With the SimSpace lab, interviewees noted this task was eliminated entirely. The VP, incident response leader at the credit card processing organization summarized: “Pretty much all of our detections are first built in the SimSpace and then ported over [to production]. It is an integral part of that detection engineering process to build detections and test the detections [in the lab] to eliminate conflicts between security operations and detection engineering.”

Modeling and assumptions. Forrester assumes the following about the composite organization:

- The detection engineering team develops 50 new detections per month.
- Engineers save 30 minutes per detection by testing these detections in the SimSpace lab environment.
- The fully burdened annual salary for a cybersecurity professional is $136,282. This is an hourly rate of $68.

Risks. The expected financial impact of this benefit is subject to risks and variation based on the following factors:

- The number of data sources and systems being monitored.
- The complexity of detection rules, quality of data sources, and the organization’s overall security posture.
- Salaries and burden rates.

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 $46,000.

Time Savings From Developing Threat Detections In Lab Environment					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
E1	Number of detections per month	Interviews	50	50	50
E2	Production time saved per detection (hours)	Interviews	0.5	0.5	0.5
E3	Number of hours saved per year	E1*E2*12	300	300	300
E4	Fully burdened hourly rate for a cybersecurity engineer	TEI standard	$68	$68	$68
Et	Time savings from developing threat detections in lab environment	E3*E4	$20,400	$20,400	$20,400
	Risk adjustment	↓10%			
Etr	Time savings from developing threat detections in lab environment (risk-adjusted)		$18,360	$18,360	$18,360
	Three-year total: $55,080			**Three-year present value: $45,659**	

Interview Spotlight: Cybersecurity Education

The education organization used SimSpace solely for cybersecurity training programs, including degree programs and executive leadership training. They said their organization first turned to SimSpace during the COVID-19 pandemic with a need to quickly pivot their in-person programs to fully online. After in-person classes resumed, their organization continued to offer classes online and subsequently increased enrollment seven-fold, as compared to pre-pandemic. In addition to these topline gains, the SimSpace training range provided some prepackaged modules, which reduced instructor course development time and enabled instructors to more effectively assess their students with range-monitoring tools. The interviewee noted that graduates of the program were highly prepared to work in companies using SimSpace.

"[SimSpace has] provided us the ability to quickly scale to support exponential growth. They have been a good partner for the past six years. They've listened to our requirements and have responded to our needs."

PROFESSOR, EDUCATION

UNQUANTIFIED BENEFITS

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

- **Range training exercises create high levels of satisfaction and confidence among teams.** Interviewees noted the realistic and interactive nature of SimSpace cyber drills led to increased employee engagement and satisfaction. Employees often appreciated the opportunity to develop and hone their skills in a controlled environment, which boosted their confidence and job satisfaction. The collaborative nature of the exercises improved team dynamics and fostered a sense of camaraderie, positively impacting overall morale.

- **The existence of a cyber range environment helps attract and retain highly qualified hires.** Interviewees reported enhanced employee morale and satisfaction from training exercises, which helped reduce turnover and the corresponding costs associated with hiring and onboarding new staff. The VP of cybersecurity engineering at the mortgage financing organization said they used the cyber drill exercises to identify strong performers, who were then recognized and rewarded, boosting retention of key employees. This interviewee stated, "You uncover those diamonds in the rough, those folks that can be superstars, and then build retention plans around them." The VP, incident response leader at the credit card processing organization mentioned finding the SimSpace cyber range to be attractive to new-hire candidates. They stated: "A lot of techie folks, who really want to get in the weeds, love having the range. So, it's been a fantastic recruiting tool for us."
- **Regular training exercises enable testing and refinement of incident response playbooks.** Interviewees from organizations in the study that employed regular exercises reported that they created a mechanism for continuous feedback loops, which helped identify and address weaknesses in their incident response playbooks. The insights gained from SimSpace after-action reviews led to the refinement of these playbooks, ensuring they are up to date in handling real-world threats. The director of information security at the insurance and investment organization stated: "[Honestly], we didn't feel fully ready or trained to handle an incident. So, it was about being prepared and testing our incident response plans."
- **Output from training exercises saves time and provides critical evidence for regulators and auditors.** The after-action reports SimSpace generated helped demonstrate preparedness to regulators and supported compliance efforts. This also reduced the time spent on regulatory audits at the interviewees' organizations due to better documentation and streamlined processes.
- **Detection engineering teams build and test detection rules and alerts before porting them over to production.** Interviewees noted that a common use of the SimSpace lab was to test and validate detection rules and alerts to ensure their accuracy and effectiveness. As the VP, incident response leader, credit card processing noted, their organization develops detections for new vulnerabilities against certain applications, sometimes beating vendor and open-source solutions by days. They

explained that the rapid response capability was critical for minimizing the impact of emerging threats.

> "We now have a master playbook and subplaybooks for major threats, developed and tested through our exercises with SimSpace."
>
> HEAD OF VULNERABILITY AND PATCH MANAGEMENT, FINANCIAL SERVICES

> "We're able to get something out to [production] generally in less than 24 hours. We have not been able to replicate that with any [hunt-and-detection] vendor solution or open-source research. While that may only happen three to four times a year, the time to value we get there is significant."
>
> VP, INCIDENT RESPONSE LEADER, CREDIT CARD PROCESSING

FLEXIBILITY

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

- **Security tool proof of concepts (POCs).** Interviewees noted a natural extension of a lab environment was testing new security tools before purchase to understand the impact they would have on threat prevention and detection. This was something most of the interviewees' organizations planned to employ. The director of information security at

the insurance and investment organization commented: “We’ve had a lot of outreach from other teams regarding POCs. … It’s beneficial to voice our capabilities and offer support to other teams within [our organization].”

- **Prepackaged training modules.** According to interviewees, SimSpace provided a limited number of training modules within their platform. Interviewees noted their organizations had just begun to explore their content and use, but plan on integrating them into other training programs.
- **Cyber insurance.** By providing better preparedness against cyberattacks, SimSpace provided the interviewees’ organizations with a rationale for lower cyber insurance premiums. Some interviewees noted their organizations recognized this and had begun conversations with their insurance carriers.

Beyond the use cases described in this report, SimSpace cyber ranges can be used in other ways, such as the following:

- **Training and assessments**. In addition to the benefits outlined in the report, organizations can use SimSpace for individual training and hiring assessments. The range can be leveraged to assess candidates in the hiring process and further build their capabilities through tailored hands-on exercises once on board.
- **Technology stack and process optimization.** SimSpace cyber range simulations can mirror customer environments to test potential use of tooling, validate security stack decisions, perform technology bakeoffs, or enhance incident response playbook development.
- **Threat intelligence research**. Cyber range environments can be used to mirror customer infrastructure and emulate research related activities, such as malware detonation, deception lab deployment, exploit development & testing, adversary emulation, device/network forensics, and vulnerability research.
- **Capability enablement**. SimSpace can support the development and optimization of customer business capabilities, such as sales support activities, R&D activities, product development, cyber insurance support, artificial intelligence/large language model product development support, or penetration testing capabilities.
- **Disaster recovery preparedness**. The SimSpace cyber range provides a simulation environment that can replicate an organization’s entire information technology and

operational technology infrastructure. This allows organizations to test disaster recovery plans without impacting production environments.

Additional information on SimSpace use cases not encountered as part of this research may be found on the SimSpace website.

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

> "The future is bright with SimSpace. We can use it for purple team exercises, decision-making for security engineering, and malware analysis. We're not doing this today, but we [plan to] get there in the next year or two."
>
> DIRECTOR OF INFORMATION SECURITY, INSURANCE AND INVESTMENT

> "Having a robust training and exercise program, which includes SimSpace, has shown our maturity as an organization. This goes into the cyber insurance assessment, which ultimately affects our [insurance] rates."
>
> DIRECTOR OF INFORMATION SECURITY, INSURANCE AND INVESTMENT

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	Annual subscription fees	$0	$525,000	$525,000	$525,000	$1,575,000	$1,305,597
Gtr	Maintenance of cyber range and planning for events	$9,724	$60,782	$60,782	$60,782	$192,070	$160,880
Htr	Annual travel costs for cyber drill events	$0	$99,000	$99,000	$99,000	$297,000	$246,198
	Total costs (risk-adjusted)	$9,724	$684,782	$684,782	$684,782	$2,064,070	$1,712,675

ANNUAL SUBSCRIPTION FEES

Evidence and data. Interviewees noted that SimSpace fees were based upon its various use cases. Among the interviewees' organizations, fees ranged broadly based on concurrent users and virtual machines (VMs). Contracts could also be single year or multiple years. Contact the vendor for more specifics.

Modeling and assumptions. For the composite organization, Forrester assumes a single year contract fee of $500,000. This includes the following parameters and services:

- SaaS licenses for up to 300 VMs and 60 concurrent users
- Professionally assisted semiannual virtual events (up to two 8-hour events)
- Access to an up-to-date full training library and attack catalog
- Introductory platform training (up to 10 seats) and range engineer training (up to four seats)
- Remote technical support

Risks. Subscription fees will vary due to use cases and deal sizes.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.3 million.

Annual Subscription Fees						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
F1	Subscription fee	Vendor		$500,000	$500,000	$500,000
Ft	Annual subscription fees	F1		$500,000	$500,000	$500,000
	Risk adjustment	↑5%				
Ftr	Annual subscription fees (risk-adjusted)		$0	$525,000	$525,000	$525,000
	Three-year total: $1,575,000			**Three-year present value: $1,305,597**		

MAINTENANCE OF CYBER RANGE AND PLANNING FOR EVENTS

Evidence and data. Interviewees' organizations allocated anywhere from less than one resource to two full-time resources for managing the cyber range and preparing for events. Their responsibilities included:

- Configuring the cyber range to mimic the production environment.
- Ensuring all necessary tools (with appropriate licenses) are available and functioning in the range. The director, information security noted challenges with obtaining licenses for some security tools.
- Developing detailed plans for the cyber drill, including objectives and scenarios, and providing training to participants on the tools and procedures. These activities were performed in conjunction with SimSpace.
- Leading the execution of the cyber drill and ensuring all objectives were met.

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

- Two engineers are assigned at 20% to perform range maintenance activities. These same resources spend two weeks planning for the initial cyber drill event.

- Salary expenses include a 35% overhead burden rate to cover benefits and payroll taxes.

Risks. The cost of maintenance of cyber range and planning for events will vary due to:

- The number and time allocation of resources assigned to manage the cyber range will vary based on the use case. Some of these responsibilities may be assumed by the vendor.
- Salaries and burden rates.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $161,000.

> "We just have a few shared stakeholders that are responsible for the lab and working with SimSpace when there is an issue. That requires some level of knowledge of how the things are architected to be able to notice when there is a problem. It's probably five to ten hours a month spread across three to four analysts."
>
> VP, INCIDENT RESPONSE LEADER, CREDIT CARD PROCESSING

Maintenance Of Cyber Range And Planning For Events						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
G1	Number of cybersecurity analysts	Interviews	2	2	2	2
G2	Fully burdened annual salary for a cyber security analyst	TEI standard	$110,511	$110,511	$110,511	$110,511
G3	Percentage of time spent on maintenance and planning activities	Interviews	4%	25%	25%	25%
Gt	Maintenance of cyber range and planning for events	G1*G2*G3	$8,841	$55,256	$55,256	$55,256
	Risk adjustment	↑10%				
Gtr	Maintenance of cyber range and planning for events (risk-adjusted)		$9,724	$60,782	$60,782	$60,782
	Three-year total: $192,070			**Three-year present value: $160,880**		

ANNUAL TRAVEL COSTS FOR CYBER DRILL EVENTS

Evidence and data. While most interviewees noted travel for cyber drill events was not required for their staff, two interviewees said their organizations found value in bringing staff together for each full-scale event. These benefits included better communication; improved team coordination among red, blue, and purple teams; and stronger team dynamics.

- These two interviewees noted their organizations had between 25% and 40% of their total staff travel to the headquarters for one week for each event.
- The other interviewees, whose organizations conducted smaller, focused events or lab use cases, noted they had no travel expenses associated with the SimSpace ranges.
- One interviewee reported that their organization also used the in-person event to allow senior executives to observe.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite has 150 security FTEs and 15% travel to the composite organization's headquarters for two events each year.
- Full-scale events last one week, including time for prebriefing and postmortems.
- The average travel cost per person is $2,000 per event.

Risks. The annual travel costs for cyber drill events will vary due to:

- The number of FTEs involved in each event.
- Distances traveled.
- Location.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $246,000.

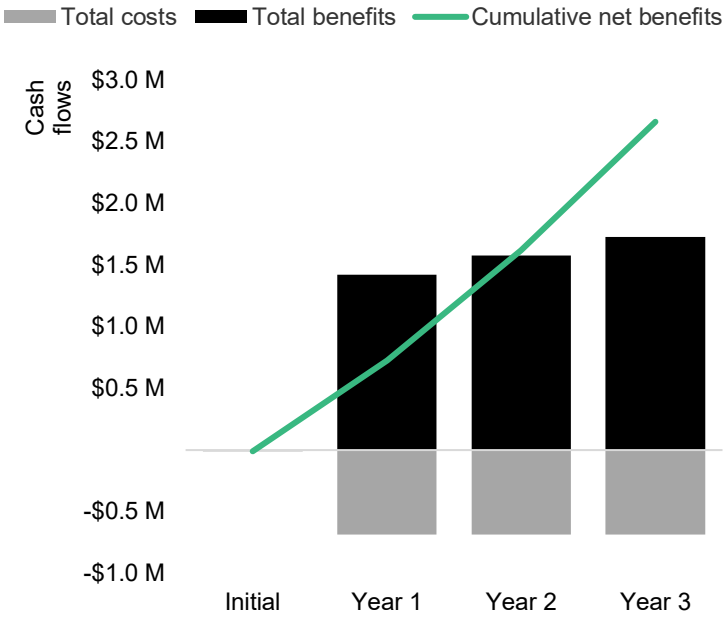
> "With most companies now remote or some hybrid version of it, this is a great reason for me to get people into [our headquarters location] to build trusted relationships. Once they realize this is not [an exercise] where we're going to use results to hold you accountable [but instead] we want to get better, they find it really fun."
>
> VP, CYBERSECURITY ENGINEERING, MORTGAGE FINANCING

Annual Travel Costs For Cyber Drill Events						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
H1	Number of FTEs involved in cyber drill	Interviews		150	150	150
H2	Percentage of FTEs who travel to event location	Interviews		15%	15%	15%
H3	Average cost of FTE travel	Assumption		$2,000	$2,000	$2,000
H4	Number of events per year	Composite		2	2	2
Ht	Annual travel costs for cyber drill events	H1*H2*H3*H4	$0	$90,000	$90,000	$90,000
	Risk adjustment	↑10%				
Htr	Annual travel costs for cyber drill events (risk-adjusted)		$0	$99,000	$99,000	$99,000
	Three-year total: $297,000			**Three-year present value: $246,198**		

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	($9,724)	($684,782)	($684,782)	($684,782)	($2,064,070)	($1,712,675)
Total benefits	$0	$1,420,801	$1,574,881	$1,728,961	$4,724,643	$3,892,186
Net benefits	($9,724)	$736,019	$890,099	$1,044,179	$2,660,573	$2,179,511
ROI						127%
Payback						<6 months

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.

Total Economic Impact Approach

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 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 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 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."

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.

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.

APPENDIX B: SUPPLEMENTAL MATERIAL

Related Forrester Research

The Forrester Wave™: Cybersecurity Skills And Training Platforms, Q4 2023, Forrester Research, Inc., December 12, 2023.

Online Resources

More information about cyber ranges is available from NIST NICE Community Coordinating Council, The Cyber Range: A Guide

APPENDIX C: ENDNOTES

[1] 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.

[2] Source: Forrester's Security Survey, 2024. Base: 84 security decision-makers with network, data center, app security, or security ops responsibilities at financial services companies with $1B+ in annual revenue. Forrester annually assesses cybersecurity metrics through interviews, surveys, and expertise in the field. Analyses are provided with information rooted with specific data sets most accurately applied to the situations that have been collected in the study.

[3] Source: Forrester's Security Survey, 2024. Base: 420 security decision-makers with network, data center, app security, or security ops responsibilities at financial services companies with $1B+ in annual revenue. Forrester annually assesses cybersecurity metrics through interviews, surveys, and expertise in the field. Analyses are provided with information rooted with specific data sets most accurately applied to the situations that have been collected in the study.

[4] Source: Forrester's Security Survey, 2024. Base: 424 security decision-makers with network, data center, app security, or security ops responsibilities at financial services companies with $1B+ in annual revenue. Forrester annually assesses cybersecurity metrics through interviews, surveys, and expertise in the field. Analyses are provided with information rooted with specific data sets most accurately applied to the situations that have been collected in the study.

[5] Source: Forrester's Security Survey, 2024. Base: 420 security decision-makers with network, data center, app security, or security ops responsibilities at financial services companies with $1B+ in annual revenue. Forrester annually assesses cybersecurity metrics through interviews, surveys, and expertise in the field. Analyses are provided with information rooted with specific data sets most accurately applied to the situations that have been collected in the study.

[6] Source: Forrester's Security Survey, 2024. Base: 221 security decision-makers with network, data center, app security, or security ops responsibilities at financial services companies with $1B+ in annual revenue. Forrester annually assesses cybersecurity metrics through interviews, surveys, and expertise in the field. Analyses are provided with information rooted with specific data sets most accurately applied to the situations that have been collected in the study.

[7] Source: Forrester's Security Survey, 2024. Base: 424 security decision-makers with network, data center, app security, or security ops responsibilities at financial services companies with $1B+ in annual revenue. Forrester annually assesses cybersecurity metrics through interviews, surveys, and expertise in the field. Analyses are provided with information rooted with specific data sets most accurately applied to the situations that have been collected in the study.

[8] Source: Forrester's Security Survey, 2024. Base: 420 security decision-makers with network, data center, app security, or security ops responsibilities at financial services companies with $1B+ in annual revenue. Forrester annually assesses cybersecurity metrics through interviews, surveys, and expertise in the field. Analyses are provided with information rooted with specific data sets most accurately applied to the situations that have been collected in the study.

[9] Source: Forrester's Security Survey, 2024. Base: 221 security decision-makers with network, data center, app security, or security ops responsibilities at financial services companies with $1B+ in annual revenue. Forrester annually assesses cybersecurity metrics through interviews, surveys, and expertise in the field. Analyses are provided with information rooted with specific data sets most accurately applied to the situations that have been collected in the study.

FORRESTER®