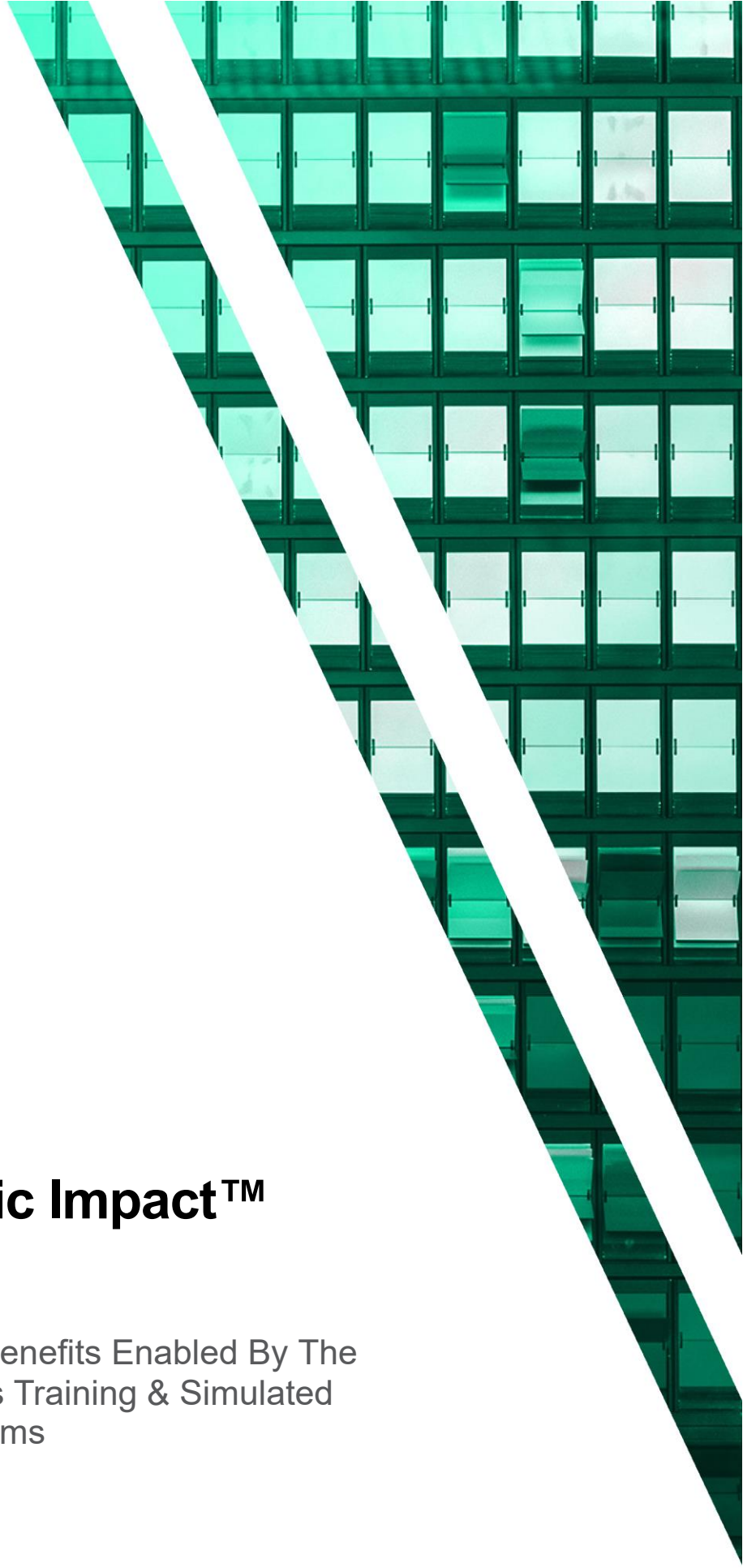
FORRESTER®



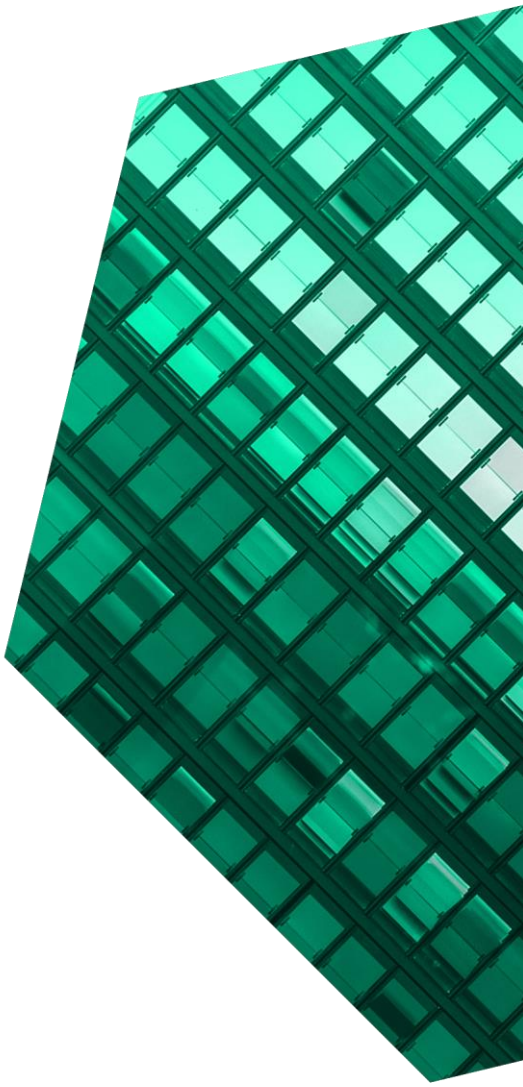
The Total Economic Impact™ Of KnowBe4

Cost Savings And Business Benefits Enabled By The KnowBe4 Security Awareness Training & Simulated Phishing And PhishER Platforms

April 2021

Table Of Contents

Consulting Team: Anna Orban
Joe Branca



ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. For more information, visit forrester.com/consulting.

Executive Summary

Anti-phishing training and simulation platforms educate users to recognize and avoid phishing emails that use social engineering to compromise targets. KnowBe4 trains and tests employees using the most current real-world scenarios as part of an ongoing program, enabling organizations to build strong human shields against cybercrime. In addition to taking the load of creating effective cybersecurity training and phishing simulation programs off the shoulders of security teams, KnowBe4's PhishER reliably automates the most time-consuming steps involved in daily user-reported email alert response and mitigation.

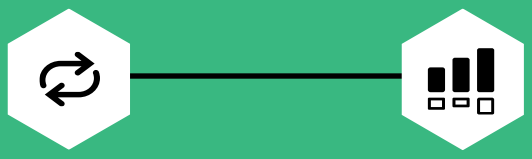
KnowBe4 commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying the KnowBe4 Security Awareness Training & Simulated Phishing and PhishER platforms. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of KnowBe4 on their organizations.

KnowBe4 is an integrated platform for security awareness training combined with simulated phishing attacks. PhishER is KnowBe4's lightweight security orchestration, automation, and response (SOAR) platform, which allows incident response teams to manage high volumes of potentially malicious email messages that users report, and it enables them to respond to the most dangerous threats more quickly and more efficiently.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed the IT security awareness program manager at a global chemical manufacturing company with more than 10,000 computer users. Forrester used this testimony to create a three-year financial analysis.

In the year prior to implementing the KnowBe4 Security Awareness Training & Simulated Phishing platform, the organization experienced various security breaches. One breach prompted a five-day manufacturing plant shutdown, while another led to a two-day malware-caused production outage in one of its labs. Also, the organization's accounts payable department kept receiving fraudulent invoices on behalf of vendors that have been compromised and one of the organization's executives became the target of a phishing attack. Decision-makers wanted to tackle the problem right where they saw that most threats could be shielded off — at the user level — by instituting a cybersecurity awareness program that would sustainably improve the organization's overall security posture.

KEY STATISTICS



Return on investment (ROI)
276%

Net present value (NPV)
$826,172

Since investing in KnowBe4 three years ago and rolling out initial baselining and ongoing training to its global user base, the organization's Phish-Prone Percentage (KnowBe4's failure indicator of users who click on phishing emails) has dropped from 19.2% to 2.8%, and the organization has not experienced cybersecurity incident-related outages or plant shutdowns on the scale that it previously did.

KEY FINDINGS

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

- **Reduction in risk exposure through a stronger cybersecurity posture, valued at $432,346 over three years.** The interviewee's organization was successful in creating a human firewall by implementing KnowBe4 Security Awareness Training & Simulated Phishing. Its low Phish-Prone Percentage rate of 2.8% is a testament of this success, and the organization has not had an outage caused by a security incident since implementing KnowBe4.

Reduced risk exposure

$432,346

- **Time savings from automated email alert notification and response, valued at $411,302.** Using KnowBe4's Phish Alert Button, the organization's employees report up to 2,000 suspicious emails in PhishER per month. About 88% of the user-reported emails are spam or threats. PhishER helps the organization manage, escalate, and remediate these large volumes of reported emails, and it also uses the PhishRIP email quarantine function to automatically quarantine and delete reported phishing emails from the mailboxes of all affected users. By automating the email incident response process, PhishER saves the organization's incident response team an average of 25 minutes of investigation/remediation work per email.
- **Cost avoidance from leveraging KnowBe4's cybersecurity training content library, valued at $164,177.** KnowBe4 provides prepackaged courseware about cybercrime that covers what it is, how it reaches its targets, and how individuals can protect sensitive information and their computers. Comprehensive training materials and quizzes that are always up-to-date eliminate the need for the organization to employ in-house staff and other resources to create and deliver ongoing training. According to Forrester's model, the organization avoids an annual cost of $65,000 by leveraging KnowBe4's always-fresh and relevant library of cybersecurity training content and newsletters.

> **"Our executives know the tides are changing every day. Hackers are getting smarter with the way they approach the creation of threats, and our executives appreciate that security awareness training and testing is constant work that has to continue and never stops."**
>
> *IT security awareness program manager*

- **Cost avoidance from leveraging prepackaged phishing content, valued at $70,875.** Creating, managing, and delivering 20 phishing campaigns per year to a large multilanguage audience can only be done efficiently with a platform that provides up-to-date content and helps automate the steps involved in successfully administering regular phishing simulations to a worldwide user base. For this analysis, Forrester assumes the organization pays a very low monthly cost of $1,500 for in-house development to account for the costs it avoids by leveraging the ready-to-use phishing simulation templates in KnowBe4 and its automated campaign delivery capabilities.
- **Cost avoidance from automated user onboarding/decommissioning in KnowBe4, valued at $46,977.** Because of the size of the interviewee's organization, the corresponding number of new hires, and regular employee turnover, the program manager previously spent an average of 10 hours per week running reports, manually enrolling new users in the training program, or removing offboarded employees from the training database. KnowBe4 directly integrates with Active Directory, ensuring that any user changes, additions, or removals transfer directly into the system. After the organization's

initial setup, user management in KnowBe4 became 100% automatic.

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

- **Increased collaboration between users and SecOps enabled proactive threat response and reduced IT help desk tickets and the need for IT remediation work.** Enabled by KnowBe4, the users at the interviewee's organization have become more collaborative. They can now easily report suspicious emails without having to submit IT service desk tickets, and they know the alerts will get immediate attention through PhishER. Not only does it require less IT involvement to follow up on user-reported emails, but security analysts can now instantaneously delete malicious content in hundreds of mailboxes at the same time. This prevents users from opening these emails, and it reduces the need for costly IT remediation work down the road.
- **Stronger corporate security posture helped avoid cost increases in cyberinsurance.** An organization's history of breaches or losses provides a picture of threat exposure, and it reveals areas that are vulnerable to security flaws. When determining its pricing model, an organization's insurance-policy underwriter will also examine existing cybersecurity training procedures. Since the interviewee's organization implemented KnowBe4, it strengthened its overall security posture and was able to noticeably reduce outages caused by security incidents. This provided the company with a strong case to negotiate its security insurance policy.

Costs. Risk-adjusted PV costs include:

- **KnowBe4 subscription cost of $252,107 over three years.** KnowBe4 licensing is based on the number of users served. The interviewee's organization added PhishER in Year 3 with a user-based subscription cost.
- **Internal labor and program operation costs of $23,216.** After the initial setup and fine-tuning of the system, the ongoing cost to manage and run training campaigns and phishing tests and to create custom reports is minimal.

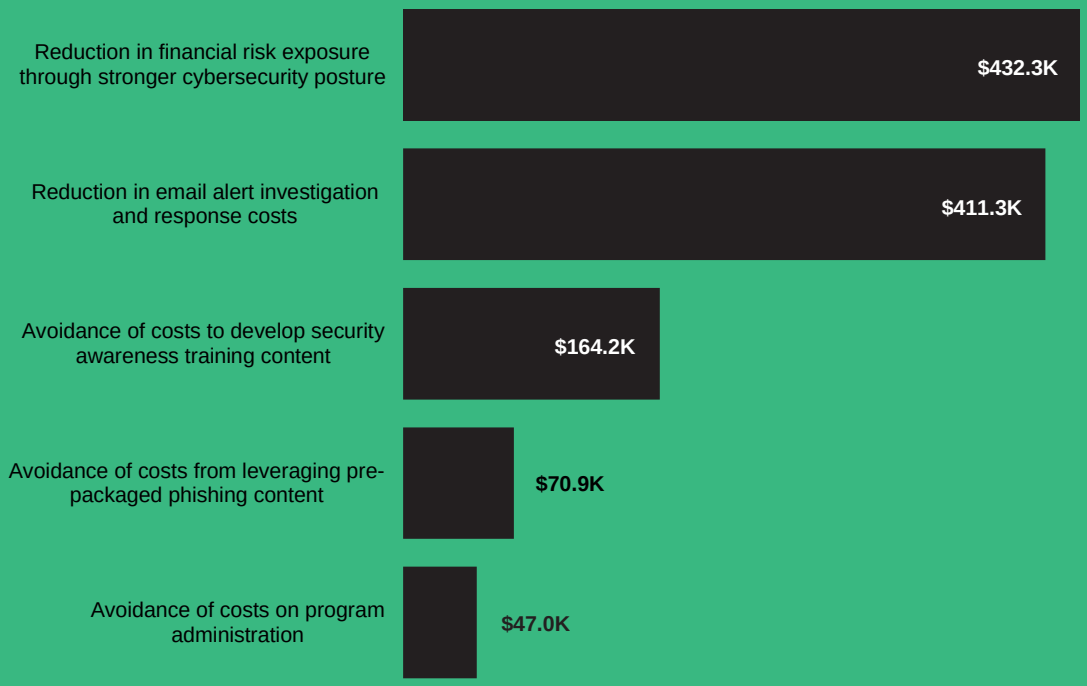
The interview and financial analysis found that this organization experiences benefits of $1,125,677 over three years versus costs of $299,505, adding up to a net present value (NPV) of $826,172 and an ROI of 276%.

"With KnowBe4 and PhishER, we have much more user trust, collaboration, and engagement. We are now way more proactive at fending off cyberthreats."

— IT security awareness program manager

ROI	BENEFITS PV	NPV	PAYBACK
276%	**$1.1M**	**$826K**	**<3 months**

Benefits (Three-Year)



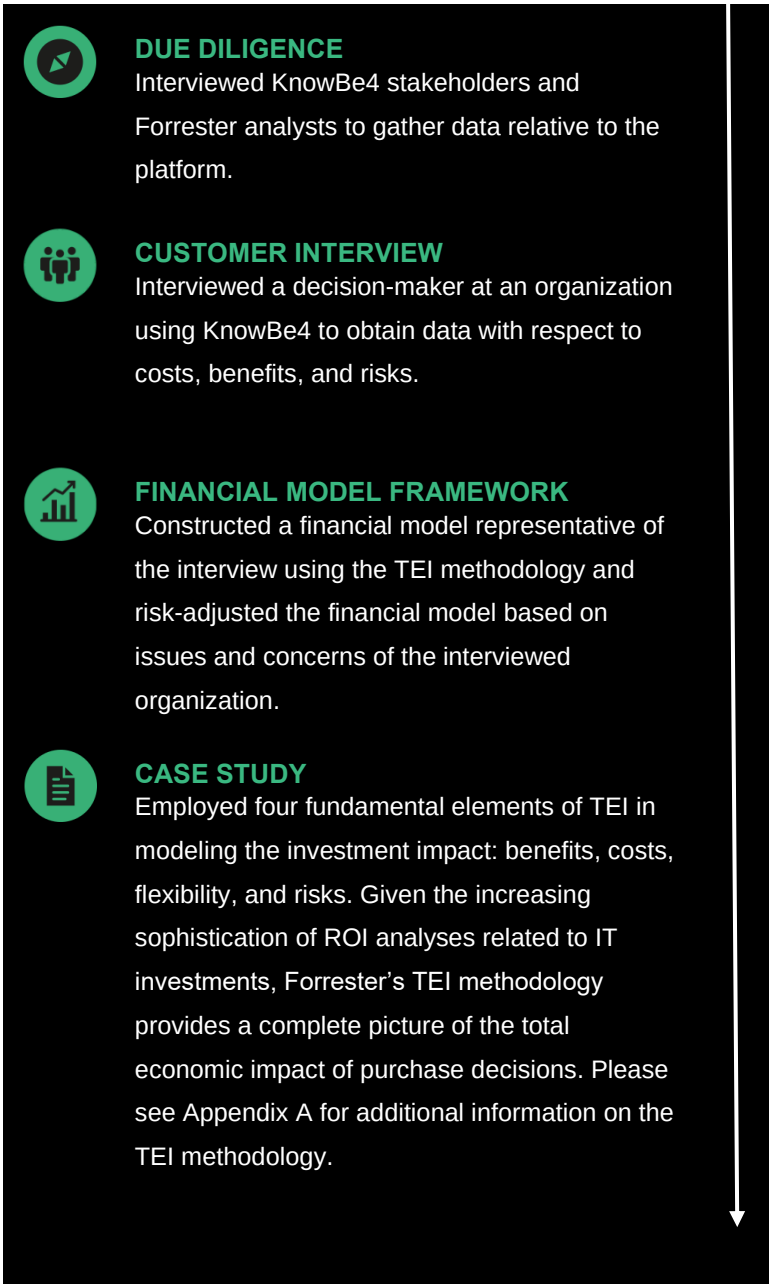
> **"People now know who the security team is and how to reach out to us. We have seen a company culture change, and I think that was the most important thing for us."**

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 KnowBe4.

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 KnowBe4 can have on an organization.

Forrester Consulting conducted an online survey of 351 cybersecurity leaders at global enterprises in the US, the UK, Canada, Germany, and Australia. Survey participants included managers, directors, VPs, and C-level executives who are responsible for cybersecurity decision-making, operations, and reporting. Questions provided to the participants sought to evaluate leaders' cybersecurity strategies and any breaches that have occurred within their organizations. Respondents opted into the survey via a third-party research panel, which fielded the survey on behalf of Forrester in November 2020.



DISCLOSURES

Readers should be aware of the following:

This study is commissioned by KnowBe4 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 the KnowBe4 platforms.

KnowBe4 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.

KnowBe4 provided the customer name for the interview but did not participate in the interview.

The KnowBe4 Customer Journey

Drivers leading to the KnowBe4 investment

INTERVIEWED ORGANIZATION

Forrester interviewed a decision-maker from an organization with experience using KnowBe4. The organization has the following characteristics:

- Global chemical manufacturing company.
- More than 170 subsidiaries and production plants.
- 10,000 computer users worldwide.

KEY CHALLENGES

After experiencing a series of production outages related to cybersecurity incidents, decision-makers with the interviewee's organization identified a lack of a dedicated security awareness training (SAT) initiative as the biggest gap in its information security program. Employees typically had difficulties recognizing phishing emails and online threats, and their ability to report such incidents was generally limited.

The interviewee spoke about several cybersecurity incidents their organization endured, including:

- In 2017, a user at a global manufacturing plant opened a malicious email attachment that led to the shutdown of the entire plant for five days.
- A lab user opened an attachment in a malicious email that infected and decommissioned all other computers in that lab. The small, local IT team worked two full days to reimage the 15 infected computers.
- More than once, hackers tried to get employees in the accounts payable department to pay fake invoices on behalf of vendors and customers whose users had been compromised.

The program manager told Forrester: "Before we implemented the security awareness training program, we just kept seeing instances of our users opening email attachments, and we had to clean all the computers that got infected. It was becoming a lot of work for our team to do all those repairs."

It was apparent that the lack of cybersafety awareness among the organization's employees was compromising its resilience to cyberthreats.

> **"Close to three years ago, our C-suite implemented KnowBe4. And since we have been in this program, we have not had a security incident like that."**
>
> *IT security awareness program manager*

INVESTMENT OBJECTIVES

The organization's decision-makers searched for a security awareness training platform that could:

- Help employees recognize phishing emails and scam advertisements to provide a strong human shield against cybercrime.
- Teach users what to do and what *not* to do when presented with suspicious messages and links, in order to improve the organization's security posture.
- Meet compliance requirements by consistently and reliably delivering SAT in every required language to employees around the world.

Additionally, the organization's decision-makers were interested in implementing capabilities for automated email incident response. They wanted to:

- Allow for the incident response team to cut through the email-alert inbox noise and to manage user-reported messages accurately and efficiently.

- Automate message prioritization, notification, escalation, and threat removal to free up time.
- Respond to the most dangerous threats more quickly and effectively.

USE CASE DESCRIPTION

Decision-makers from the interviewee's organization chose KnowBe4 for what they perceived to be the superior technology the platform offers and because of KnowBe4's extensive cybersecurity training content, which is always fresh and up-to-date about current cyberthreats. The internal evaluation team also found KnowBe4's training content and testing quizzes to be very user-friendly and engaging.

A new IT security awareness program manager was recruited to oversee the KnowBe4 platform, to coordinate the cybersecurity training and phishing campaigns, and to oversee a team of IT security analysts that handles user-reported email alerts.

The company has about 10,000 users who have an email address, making them eligible to receive training and phishing simulations via KnowBe4. The other 600 plant employees who have no specific email addresses but who have access to computers receive security-awareness posters and other useful printouts to ensure this user group receives ongoing security awareness training as well.

Phish-Prone Percentage rate dropped from the initial **19.2%** to only **2.8%**.

To augment the organization's security awareness program, the SAT team implemented KnowBe4's PhishER capability, which uses automation and machine learning through PhishML to help security alert investigation and response teams to manage the email alert inbox and to efficiently remediate security threats.

"With PhishER, we have seen so many real threats being reported by users because they now know how to report suspicious emails," said the IT security awareness program manager. "We don't have to wait to assign requests to the IT help desk; we can just go ahead and take action through PhishER."

For this use case, which includes KnowBe4's Security Awareness Training & Simulated Phishing and PhishER platforms, Forrester has modeled benefits and costs over three years.

> **"KnowBe4 is constantly updating its training content to be relevant to real, current cyberthreats and events in the world. I always send the most up-to-date cybersecurity training to my users, and they love it."**
>
> — IT security awareness program manager

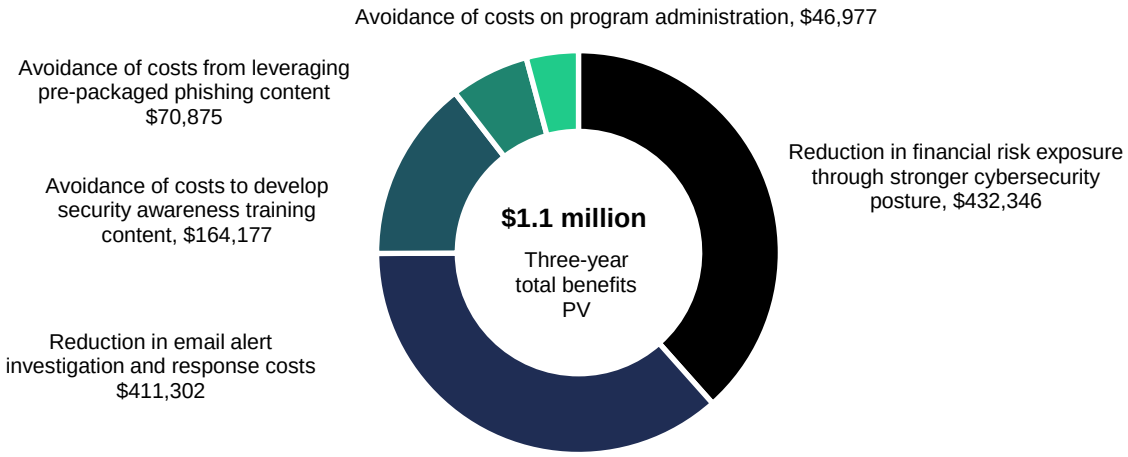
Analysis Of Benefits

Quantified benefit data

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Reduction in financial risk exposure through stronger cybersecurity posture	$161,078	$181,213	$181,213	$523,505	$432,346
Btr	Reduction in email alert investigation and response costs	$146,337	$165,969	$187,810	$500,116	$411,302
Ctr	Avoidance of costs to develop security awareness training content	$65,769	$66,032	$66,303	$198,105	$164,177
Dtr	Avoidance of costs from leveraging pre-packaged phishing content	$28,500	$28,500	$28,500	$85,500	$70,875
Etr	Avoidance of costs on program administration	$0	$29,355	$30,236	$59,591	$46,977
	Total benefits (risk-adjusted)	$401,684	$471,069	$494,062	$1,366,817	**$1,125,677**

The table above shows the total of all benefits across the areas listed in this section, as well as present values (PV) discounted at 10%. Over three years, the interviewee's organization expects risk-adjusted total benefits to have a PV of more than 1.1 million.

Benefits by category



This section examines five quantified benefits and provides insight into the data points and evidence collected during the customer interview as well as the underlaying models and assumptions used in the financial analysis for this use case.

REDUCTION IN FINANCIAL RISK EXPOSURE THROUGH STRONGER CYBERSECURITY POSTURE

Evidence and data. The interviewee's organization reduced the likelihood of costly security breaches through user training.

- After rolling out KnowBe4, the security team has been able to provide continuous reinforcement of safe security techniques to its user base and improve their awareness of the risks of phishing emails and other online threats.
- Taking a more proactive approach to cybersecurity, the organization has become more resilient against cyberthreats, and decision-makers can take pride in the low corporate Phish-Prone Percentage rate of 2.8%.
- The program manager said, "Since we implemented our program, we haven't had any more outages or incidents that would have resulted in financial losses."

Modeling and assumptions. Forrester used the following data to model the financial value of this benefit for the interviewee's organization:

- According to Forrester Consulting's Cost Of A Cybersecurity Breach survey, the average cost of a security breach at an enterprise-size organization is $658,000, and the average number of security breaches resulting in financial loss is 1.7 per year.[1]
- This model assumes that 40% of security incidents are avoidable by implementing a strong human firewall. To be conservative, this analysis attributes just 45% of the total risk reduction to KnowBe4, ramping up from 40% in Year 1.

Risks. Risks that may affect an organization's ability to reduce its risk exposure and avoid financial losses include the employees' abilities to recognize and report potential security threats and to apply safe email and online security techniques.

To account for this risk, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of **$432,346**.

Reduction In Financial Risk Exposure Through Stronger Cybersecurity Posture

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
A1	Total cost of a security breach (average external and internal costs per year)	Forrester Consulting Cybersecurity survey	$658,000	$658,000	$658,000
A2	Average number of security breaches resulting in material losses per year	Forrester Consulting Cybersecurity survey	1.7	1.7	1.7
A3	Average total annual cost of security breaches per organization	A1*A2	$1,118,600	$1,118,600	$1,118,600
A4	Percent of breaches avoidable through a stronger human firewall	Assumption	40%	40%	40%
A5	Average annual cost of breaches avoidable with stronger human firewall	A3*A4	$447,440	$447,440	$447,440
A6	Percent attributed to KnowBe4	Assumption	40%	45%	45%
At	Reduction in financial risk exposure through stronger cybersecurity posture	A5*A6	$178,976	$201,348	$201,348
	Risk adjustment	↓10%			
Atr	Reduction in financial risk exposure through stronger cybersecurity posture (risk-adjusted)		$161,078	$181,213	$181,213
	Three-year total: $523,505			**Three-year present value: $432,346**	

REDUCTION IN EMAIL ALERT INVESTIGATION AND RESPONSE COSTS

Evidence and data. By automating email security remediation workflows, the interviewee's organization reduced the amount of time it spends on these tasks.

- Prior to the implementation of KnowBe4's Phish Alert Button and PhishER, users reported suspicious emails for the IT security team to manually filter through. Lacking automated escalation and email quarantine and removal capabilities, the process of investigating and remediating potential security threats was inconsistent, time-consuming, and error-prone.
- With PhishER the organization's small security team could efficiently manage, escalate, and remediate large volumes of reported emails, and use the PhishRIP function to quickly shut down active phishing attacks.

Modeling and assumptions. Forrester used the following data to model the financial value of this benefit for the interviewee's organization:

- On average, users report 1,600 suspicious emails each month, and this increases 10% year over year.
- PhishER reduces the average effort required for email alert follow-up and remediation from 30 minutes to 10 minutes per user-reported email.
- Time savings for the organization adds up to more than 500 hours per month. Forrester applied a 50% adjustment to reported time savings to produce a conservative estimate of employee time rededicated to productive tasks.

Risks. Risks that may affect the creation of a more efficient email alert response process include:

- Employees' buy-in to report suspicious emails via the KnowBe4 Phish Alert Button.
- The level to which the incident response team customizes rules and actions in PhishER.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of **$411,302**.

Reduction In Email Alert Investigation And Response Costs

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
B1	Security analyst fully loaded annual salary	Year 1: Assumption Years 2 and 3: $B1_{PY}$*103%	$100,000	$103,000	$106,090
B2	Spam or malicious emails reported via the Phish Alert Button per month	Interview: 10% annual growth	1,600	1,760	1,936
B3	Time-to-resolution without automation (minutes)	Interview	30	30	30
B4	Time-to-resolution with Phish Alert Button and PhishER/PhishRIP (minutes)	Interview	10	10	10
B5	Email alert investigation hours saved per month (rounded)	B2*(B3-B4)/60	533	587	645
B6	Productivity capture rate	Assumption	50%	50%	50%
B7	Monthly time savings driving additional productivity (rounded)	B5*B6	267	294	323
Bt	Reduction in email alert investigation and response costs	(B1/2,080)*(B7*12)	$154,038	$174,704	$197,695
	Risk adjustment	↓5%			
Btr	Reduction in email alert investigation and response costs (risk-adjusted)		$146,337	$165,969	$187,810
	Three-year total: $500,116			**Three-year present value: $411,302**	

AVOIDANCE OF COSTS TO DEVELOP SECURITY AWARENESS TRAINING CONTENT

Evidence and data. By leveraging KnowBe4's training platform and its library of pre-packaged courseware on cybercrime, the interviewee's organization did not have to employ dedicated internal or external resources to research, create, and deliver ongoing security training and content to its global user base.

- Comprehensive courses and quizzes that are always up-to-date ensure ongoing cybersecurity training in all required languages.
- The IT security awareness program manager leverages KnowBe4's role-based content with users in mission-critical roles.

Modeling and assumptions. Forrester modeled savings for the interviewee's organization through out-of-the-box availability of the following types of training content:

- Weekly "Phishing Scams of the Week" newsletters available in KnowBe4 reinforce cybersecurity awareness best practices, eliminating the need for the IT security awareness program manager to invest about 4 hours per week into researching and developing this content.
- The company also leverages KnowBe4's library of cybersecurity training content to formally train its user base once every month. This analysis assumes that the organization avoids paying $5,000 per training session, 12 times per year.

Risks. Risks that may affect this benefit include the ability of the organization's program manager to utilize pre-packaged training content on a regular basis.

To account for this risk, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of **$164,177**.

Avoidance Of Costs To Develop Security Awareness Training Content

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
C1	Security analyst fully loaded annual salary	Year 1: Assumption Years 2 and 3: $C1_{PY}$*103%	$100,000	$103,000	$106,090
C2	Time saved on not having to prepare weekly security newsletter (hours)	Interview	4	4	4
C3	Number of security newsletters per year	Interview	48	48	48
C4	Time saved annually on the preparation of weekly newsletters (hours)	C2*C3	192	192	192
C5	Annual avoidance of costs to prepare weekly security newsletters (rounded)	(C1/2,080)*C4	$9,231	$9,508	$9,793
C6	Number of security awareness training sessions delivered per year	Interview	12	12	12
C7	Cost to create one training session	Assumption	$5,000	$5,000	$5,000
C8	Annual avoidance of costs to prepare engaging training content	C6*C7	$60,000	$60,000	$60,000
Ct	Avoidance of costs to develop security awareness training content	C5+C8	$69,231	$69,508	$69,793
	Risk adjustment	↓5%			
Ctr	Avoidance of costs to develop security awareness training content (risk-adjusted)		$65,769	$66,032	$66,303
	Three-year total: $198,105			**Three-year present value: $164,177**	

AVOIDANCE OF COSTS FROM LEVERAGING PRE-PACKAGED PHISHING CONTENT

Evidence and data. Leveraging ready-to-use phishing simulation templates in KnowBe4 and the platform's automated campaign delivery capabilities saved the interviewee's organization internal development and coordination time while ensuring regular phishing simulation campaign delivery throughout the year.

- The interviewee's organization can now efficiently create and deliver 20 phishing campaigns per year in multiple languages to its worldwide audience via KnowBe4. The platform provides up-to-date content and automates steps involved in administering phishing simulations to the organization's user base at more than 170 offices, production facilities, and labs around the world.
- KnowBe4 handles post-simulation user follow-up and learnings reinforcement, and it provides detailed management reports after phishing simulations. This created additional efficiencies for the SAT team.

Modeling and assumptions. Forrester used the following data to model the financial value of ready-to-use content and automated phishing simulations for the interviewee's organization:

- The organization delivers up to 20 phishing simulations to its global user base per year.
- For this business case, Forrester used a low monthly $1,500 cost of in-house development to account for the costs the organization avoids by leveraging ready-to-use phishing simulation templates and KnowBe4's automated campaign-delivery capabilities.

> **"With COVID-19, and users being more diligent about reporting emails; with PhishER we keep seeing all those new threats coming through. So, I use phishing simulations between security trainings, and sometimes even more often than that."**
>
> *IT security awareness program manager*

Risks. Risks that may affect this benefit include the ability of the IT security awareness program manager to utilize pre-packaged phishing simulation content and testing campaigns.

To account for this risk, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of **$70,875**.

Avoidance Of Costs From Leveraging Pre-Packaged Phishing Content

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
D1	Number of phishing simulations delivered per year	Interview	20	20	20
D2	Cost to create, deliver, and manage one phishing simulation campaign	Assumption	$1,500	$1,500	$1,500
Dt	Avoidance of costs from leveraging pre-packaged phishing content	D1*D2	$30,000	$30,000	$30,000
	Risk adjustment	↓5%			
Dtr	Avoidance of costs from leveraging pre-packaged phishing content (risk-adjusted)		$28,500	$28,500	$28,500
	Three-year total: $85,500			**Three-year present value: $70,875**	

AVOIDANCE OF COSTS ON PROGRAM ADMINISTRATION

Evidence and data. By automating new user onboarding and offboarding via KnowBe4's Active Directory Integration (ADI), the interviewee's organization entirely eliminated the manual effort involved with these program administration tasks.

- The IT security awareness program manager explained: "When a new employee gets added to our Active Directory, the new user gets pulled into the KnowBe4 console and is already assigned to a Smart Group called 'New Hires,' and they are automatically assigned to a specific course."

Modeling and assumptions. Forrester used the following data to model the financial value of this benefit for the interviewee's organization:

- Previously, the program manager would spend up to 10 hours per week running reports and manually enrolling new users in the training program or removing offboarded employees from the training database. KnowBe4 now directly links to Active Directory and ensures that any user changes, additions, or removals transfer directly into the system.
- At a large organization with more than 10,000 training participants, user administration can be an ongoing and time-consuming effort if done manually. After initial setup of KnowBe4, user management becomes 100% automatic.
- This efficiency benefit came into effect in the second year of the organization's KnowBe4 deployment after IT completed an Active Directory refresh project.

> **"I don't need to do anything. The platform just does that itself. Every time an employee leaves, they are removed from the system. When a new employee joins in, they're already created within the KnowBe4 console and automatically signed up to 'New Hires' training."**
>
> *IT security awareness program manager*

Risks. Risks that may affect this benefit include the need for the organization's IT security awareness program manager to organize training for computer users not registered in the company's Active Directory.

To account for this risk, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of **$46,977**.

Avoidance Of Costs On Program Administration

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
E1	Senior security analyst fully burdened annual salary	Year 1: Assumption Years 2 and 3: $E1_{PY}$*103%	$120,000	$123,600	$127,308
E2	Time saved per week on program administration (hours)	Interview	0	10	10
E3	Time saved annually on program administration (hours)	E2*52 weeks	0	520	520
Et	Avoidance of costs on program administration	(E1/2,080)*E3	$0	$30,900	$31,827
	Risk adjustment	↓5%			
Etr	Avoidance of costs on program administration (risk-adjusted)		$0	$29,355	$30,236
	Three-year total: $59,591			**Three-year present value: $46,977**	

UNQUANTIFIED BENEFITS

Additional benefits that the interviewee said their organization experienced but was not able to quantify include:

- **Increased collaboration between users and SecOps.** The IT security awareness program manager explained how the new process increased user trust and collaboration with the incident response team because users now know that the alerts they submit trigger immediate action. The interviewee said: **"**Users would report suspicious emails to an internet security solution used by the IT department, but they would never get a response back, or they would send an email to the service desk and wait a few hours to hear back. Whereas with PhishER, they get an automatic, instant email saying this was a legit email or spam or a threat."
- **Better control of cyberinsurance costs.** The interviewee said, **"**We have to prove to the auditors every year that we implemented layers of protection, because it's going to impact our insurance." Successfully implementing KnowBe4 provides the company with a strong case to negotiate its security insurance policy.

Improved user trust, collaboration, and proactive threat remediation

Attributed to KnowBe4

FLEXIBILITY

The value of flexibility is unique to each organization. There are multiple scenarios in which an organization might implement KnowBe4 and later realize additional uses and business opportunities.

For example, many countries have regulations requiring that security training be offered in the user's local language. Once the IT project to add language assignments to users in Active Directory is complete, the SAT team will be able to leverage KnowBe4's localized learning experience feature. Based on Smart Groups the program manager creates, the KnowBe4 console will automatically assign the specific language training to users. Users will be able to access their training completion statuses and achievement badges in their local languages.

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

> **"Before we had PhishER, users would just send an email to the service desk. But what could happen during those 3 to 4 hours that it could take the service desk to assign the request to the appropriate team and get back to the user?"**
>
> — IT security awareness program manager

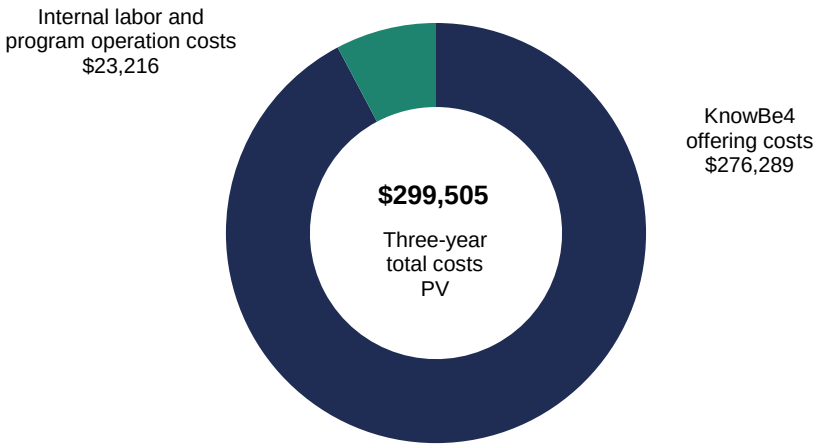
Analysis Of Costs

Quantified cost data

Total Costs						
Ref.	**Metric**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Ftr	KnowBe4 offering costs	$111,100	$111,100	$111,100	$333,300	$276,289
Gtr	Internal labor and program operation costs	$12,358	$7,487	$7,712	$27,557	$23,216
	Total costs (risk-adjusted):	$123,458	$118,587	$118,812	$360,857	**$299,505**

The table above shows the total of all costs across the areas listed in this section, as well as present values (PV) discounted at 10%. Over three years, the interviewee's organization expects risk-adjusted total costs to be a PV of $299,505.

Costs by category



This section examines the costs incurred with licensing, setting up, customizing, and managing the KnowBe4 Security Awareness Training & Simulated Phishing and PhishER platforms as implemented in this use case.

KNOWBE4 OFFERING COSTS

Evidence and data. KnowBe4 is offered as a software-as-a-service (SaaS) subscription, and it is priced per seat, per year. Three levels of training are available with varied levels of access to platform features.

- The interviewee's organization opted for a three-year Diamond-level subscription to maximize available discounts and to ensure access to Training Access Level III (which is the highest level of training) and beta program participation.
- Security Awareness Training & Simulated Phishing is licensed separately, while the PhishER platform is licensed as an optional add-on capability that integrates with the KnowBe4 Security Awareness Training & Simulated Phishing platform.

Modeling and assumptions. Forrester used the following data to model KnowBe4 fees for the interviewee's organization:

- The organization purchases 10,000 licenses for KnowBe4 Security Awareness Training & Simulated Phishing at a three-year subscription cost of $265,000. This translates to $8.83 per user per year.
- The organization purchases 10,000 licenses for PhishER separately at a three-year subscription cost of $38,000. This translates to $1.27 per user per year.
- The total current license fees for this organization are $101,000 per year for a three-year subscription to the KnowBe4 Security Awareness Training & Simulated Phishing platform and the PhishER platform.

Risks. Risks that may impact KnowBe4 subscription fees include:

- The choice of the level of subscription (e.g., Gold, Platinum, or Diamond).
- The availability of multiyear discounts on contract commitments of less than three years or on renewals.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of **$276,289**

.

KnowBe4 Offering Costs

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
F1	License cost per user for KnowBe4	Interview	$8.83	$8.83	$8.83
F2	License cost per user for PhishER	Interview	$1.27	$1.27	$1.27
F3	Total license costs per user	F1+F2	$10.10	$10.10	$10.10
F4	Users	Interview	10,000	10,000	10,000
Ft	KnowBe4 offering costs	F3*F4	$101,000	$101,000	$101,000
	Risk adjustment	↑10%			
Ftr	KnowBe4 offering costs (risk-adjusted)		$111,100	$111,100	$111,100
	Three-year total: $333,300			**Three-year present value: $276,289**	

INTERNAL LABOR AND PROGRAM OPERATION COSTS

Evidence and data. The interviewee's organization used internal labor for implementation, management, and support of the KnowBe4 platforms.

- The organization's KnowBe4 customer success manager provided informal assistance in setting up the initial reports.
- The organization's KnowBe4 customer success manager trained the IT security awareness program manager on the use of KnowBe4.

Modeling and assumptions. Forrester used the following data to model KnowBe4 fees for the interviewee's organization:

- As a cloud-based tool, KnowBe4 requires minimal ongoing management and maintenance. However, in the first year of implementation, the interviewee's organization's staff spent approximately 4 hours per month building out automations, customizing templates, ensuring the correct data went into custom fields, exploring ways to fully capitalize on KnowBe4's capabilities, and reviewing KnowBe4 analytics to find opportunities to fine-tune the security training program.
- The organization invests an average of 8 hours per month in ongoing training and phishing program planning and delivery.
- It takes an estimated 2 hours per month to set up, review, and distribute training completion and phishing test reports to management. However, during the first year of deployment, the setup and fine-tuning of reports for individual regions required an additional time investment that added up to 5 hours per month.

Risks. The time required to set up and fine-tune the KnowBe4 platform components may impact the organization's program operation costs.

To account for this risk, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of **$23,216**.

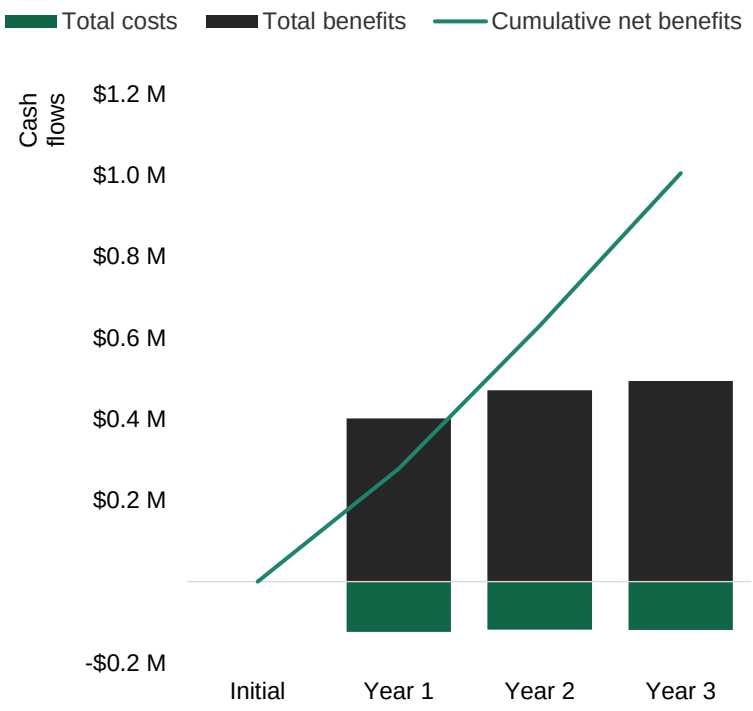
Internal Labor And Program Operation Costs

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
G1	Senior security analyst fully loaded annual salary	Year 1: Assumption Years 2 and 3: $G1_{PY}$*103%	$120,000	$123,600	$127,308
G2	Time to set up and fine-tune the KnowBe4 system (hours per month)	Interview	4	0	0
G3	Hours managing the training system and running phishing campaigns per month	Interview	8	8	8
G4	Hours creating custom reports for regions per month	Interview	5	2	2
Gt	Internal labor and program operation costs	(G1/2,080)*(G2+G3+G4)*12	$11,769	$7,131	$7,345
	Risk adjustment	↑5%			
Gtr	Internal labor and program operation costs (risk-adjusted)		$12,358	$7,487	$7,712
	Three-year total: $27,557			**Three-year present value: $23,216**	

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)

	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($123,458)	($118,587)	($118,812)	($360,857)	($299,505)
Total benefits	$401,684	$471,069	$494,062	$1,366,817	$1,125,677
Net benefits	$278,226	$352,482	$375,250	$1,005,960	$826,172
ROI					276%

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

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

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

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

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV 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.

PRESENT VALUE (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

NET PRESENT VALUE (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made, unless other projects have higher NPVs.

RETURN ON INVESTMENT (ROI)

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

DISCOUNT RATE

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

PAYBACK PERIOD

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

Appendix B: Endnotes

[1] Source: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q4 2020.


FORRESTER®