A Forrester Total Economic Impact™ Study

Commissioned By

KnowBe4

Project Director:
Reggie Lau

January 2017

The Total Economic Impact™ Of KnowBe4

Risk Mitigation And Cost Efficiencies Enabled By KnowBe4

FORRESTER®

Table Of Contents

ABOUT FORRESTER CONSULTING

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

FORRESTER®

Executive Summary

In January 2017, 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 KnowBe4. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of KnowBe4 on their organizations.

> *"We went from being 60% phish-prone in our first test to 14% in the second month — even though we tailored the second phish email to include content related to free memorabilia for a local professional sports team that recently won a national championship."*
>
> ~ Chief information security officer, large US healthcare network

According to recent studies from Verizon and IBM, 30% of recipients open phishing messages.[1] Seventy percent of executives paid to resolve ransomware hacks.[2] Per Forrester's 2016 data security report, 41% of data breaches in 2016 were due to internal incidents, making it the top cause of successful cyberattacks in 2016, rising from 39% in 2015.[3] The majority of internal incidents (65%) are mostly inadvertent in nature, stemming from staff unintentionally installing malware or providing access credentials. And even for the third (35%) of these events that are attributed to malicious insiders who intentionally steal or leak data, it's more likely that these incidents are more inadvertent in nature with staff who are targeted for data or access to data once they have already been compromised.

KnowBe4 provides organizations with security awareness training and simulated phishing solutions to mitigate the risks of these inadvertent internal cyberattacks. In addition to learning modules that can either replace or supplement a customer's legacy security awareness training content, KnowBe4 offers features to enhance the capabilities and efficiency of security testing. The solution includes key features like scheduling and automating phishing attacks, spoofing domains, targeting and reporting by organizational groups, and using and customizing phishing templates from a large selection of timely and relevant templates. It also includes a "Phish Alert" add-in button to email clients that allows end users to report suspicious emails.

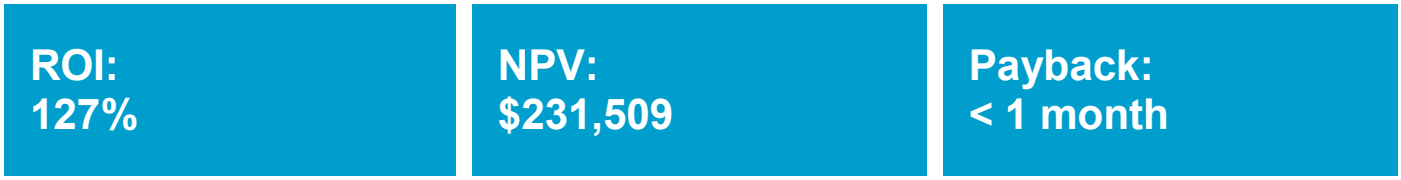
To better understand the benefits, costs, risks, and long-term flexibility associated with KnowBe4, Forrester interviewed an existing customer with at least six months of experience using the solution. Prior to adopting KnowBe4, the interviewed customer, a large US healthcare network, used internally developed content for annual security awareness training. Learnings were not typically reinforced during the year, and any complementary newsletters or internal alerts regarding a specific malware trend were reactive. As the organization's IT security team gained technical controls through hardware and software, the team realized the largest remaining vulnerability was an uninformed staff. The organization investigated different options and selected KnowBe4 for its user interface, training content, and cost effectiveness.

KNOWBE4 IS A COST-EFFECTIVE SOLUTION THAT MITIGATES RISK OF SOCIAL ENGINEERING AND ENABLES AN ORGANIZATION TO LEVERAGE ALL STAFF TO BE PART OF THE SECURITY APPARATUS

Our interview with an existing customer and subsequent financial analysis found that the interviewed organization experienced the risk-adjusted ROI, benefits, and costs shown in Figure 1.[4] See Appendix A for a description of the interviewed organization.

The interviewed customer experienced three-year, risk-adjusted benefits of $413,634 versus costs of $182,125, resulting in a net present value (NPV) of $231,509.

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



Source: Forrester Research, Inc.

› **Benefits.** The interviewed organization experienced the following three-year risk-adjusted present value benefits:

- **Mitigating risk of revenue loss, reputation loss, and increased cost of compliance.** This benefit focuses on conceptually modeling the value of risk mitigation, which is often the core component of business cases related to security. This benefit category includes metrics like stolen intellectual property (IP); downtime or loss of service resulting in missed revenue opportunities; public news of breaches causing brand and reputational damage that harms customer acquisition, retention, and enrichment; and data breaches that involve fines, penalties, and increased audit and remediation costs. Given the variability of these costs, and the intangible value of many of the elements, this study will propose the metrics and conceptual framework that readers may use to build a business case.[5] With that said, it is worth noting that many organizations today heavily rely on intangible assets — the very items information security teams are tasked with protecting — now consisting of over 80% of the S&P 500's market value.[6]
- **Reduction in breach remediation costs ($102,778).** This benefit centers on the reduction of breach events stemming from phishing attacks on users. The reduction of breaches proportionally reduces the time and effort related to remediation tasks such as workstation reimaging and server recovery. The customer highlighted that these events reduced from double digits each month prior to adopting KnowBe4 to low double digits, single digits, and finally to zero within one year of deploying KnowBe4.
- **Third-party simulation cost avoidance ($310,856).** This benefit highlights the cost effectiveness of using KnowBe4 instead of the interviewed customer's closest alternative. For the interviewed customer, this alternative involved using a third-party company to conduct periodic security awareness trainings and phishing simulations. The model assumes this type of managed security service provider (MSSP) may provide other security services and only applies a partial cost and time to the model. The customer mentioned that KnowBe4's annual solution cost is almost the same as the monthly cost of employing a third-party company to run phishing tests. The customer also mentioned the possibility of internally building out security awareness training content and the capability to simulate phishing. However, the customer mentioned this would be expensive and inefficient compared with both the MSSP alternative and the KnowBe4 solution. Readers should identify their closest realistic alternative to compare the time, effort, and investment with KnowBe4.

› **Costs.** The interviewed organization experienced the following three-year risk-adjusted present value costs:

- **KnowBe4 solution cost ($170,971).** This cost focuses on the annual license cost, which is based on services, packaging, and volume of users. This study uses an estimated cost based on the customer's total staff and subscribed services. Readers should reach out to KnowBe4 for a tailored quote based on their needs and volume.
- **Internal labor and implementation ($11,154).** This cost centers on the time and effort related to ongoing operations of the solution. The customer mentioned immaterial initial effort and about 4 total hours each month to operate both the solution and the larger security awareness program.

Disclosures

The reader should be aware of the following:

- The 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 report to determine the appropriateness of an investment in KnowBe4.
- 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 names for the customer interview but did not participate in the interview.

TEI Framework And Methodology

INTRODUCTION

From the information provided in the interviews, Forrester has constructed a Total Economic Impact (TEI) framework for those organizations considering deploying KnowBe4. The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision.

APPROACH AND METHODOLOGY

Forrester took a multistep approach to evaluate the impact that KnowBe4 can have on an organization (see Figure 2). Specifically, we:

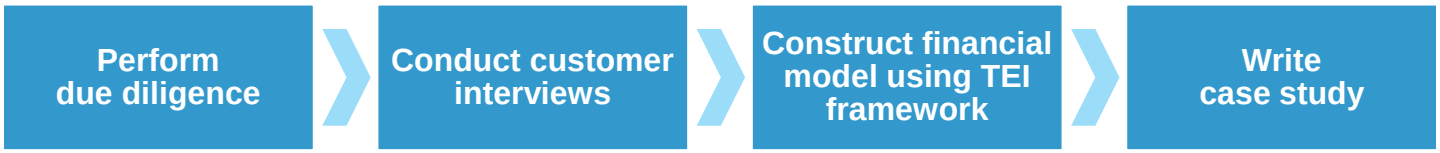
- Interviewed KnowBe4 marketing, sales, and consulting personnel, along with Forrester analysts, to gather data relative to KnowBe4's marketplace.
- Interviewed one organization currently using KnowBe4 to obtain data with respect to costs, benefits, risks, and long-term flexibility.
- Constructed a financial model representative of the interviews using the TEI methodology. The financial model is populated with the cost and benefit data obtained from the interviews.
- Risk-adjusted the financial model based on issues and concerns the interviewed organization highlighted in interviews. Risk adjustment is a key part of the TEI methodology. While the interviewed organization provided cost and benefit estimates, some categories included a broad range of responses or had a number of outside forces that might have affected the results. For that reason, some cost and benefit totals have been risk-adjusted and are detailed in each relevant section.

Forrester employed four fundamental elements of TEI in modeling KnowBe4's value: benefits, costs, flexibility, and risks.

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

FIGURE 2

TEI Approach



Source: Forrester Research, Inc.

Analysis

INTERVIEWED CUSTOMER DESCRIPTION

For this study, Forrester interviewed a large, US-based healthcare network with the following characteristics:

- Comprises 10 medical facilities.
- Has over 10,000 user accounts with 1,000 to 2,000 reserved for nonemployees such as students and contractors.
- Has an IT security team of 16 people with a budget of more than $4 million.

INTERVIEW HIGHLIGHTS

The interviewed customer highlighted the following pre-KnowBe4 issues and gaps, technology selection criteria and goals, and post-KnowBe4 deployment results.

Situation

Prior to engaging KnowBe4, the interviewed customer did not conduct phishing simulations and provided the bare essentials for annual security awareness training. There was not a lot of proactive or interactive follow-up to the once-a-year compliance training. Articles or alerts that were sent or posted on the intranet were typically reactive to security events in the news. After onboarding a new director to lead information security, the organization built out its security infrastructure and processes. Eight years later, the team had established technical controls and processes and realized that end users were the remaining weak link. The organization sought to reduce its vulnerability to social engineering threats.

Solution

The interviewed customer reviewed several options, including developing an internal awareness training and phishing simulator, employing a third party to conduct phishing tests, and adopting a platform that would allow the IT security team to plan and customize phishing simulations. The customer ultimately selected KnowBe4 based on the following criteria:

- An intuitive user interface with minimal training needed.
- Customizable phishing templates and targeting.
- Accessibility and completeness of training content.
- Cost effectiveness relative to options considered.

> *"We were experiencing double-digit remediation events each month prior to KnowBe4 and were able to bring that down to single digits quickly. We have not had to reinstall anything related to ransomware in the past year."*
>
> ~ Chief information security officer, large US healthcare network

> *"We didn't see this coming, but the Phish Alert button is amazing. We don't just get 10,000 people to function as part of the security, but also provide security intelligence."*
>
> ~ Chief information security officer, large US healthcare network

After selecting KnowBe4, the interviewed customer deployed with the following goals, which were achieved in Year 1:

- Reduce the phish-prone percentage (i.e., those who have clicked on phishing emails in the past are thus more likely to in the future) from 60% in diagnostic tests down to single-digit percentages in one year.[7]
- Increase simulation sophistication and effectiveness over time through software automation and phishing content tailored to customer organizational attributes, current events, spoofing domains, and target staff or departments
- Integrate the Phish Alert button into email and communication systems to build more intuitive reporting mechanisms for individual employees.
- Build better, more engaging security awareness content and proactive alerting reward systems to further improve security behavior via performance management and incentive systems.

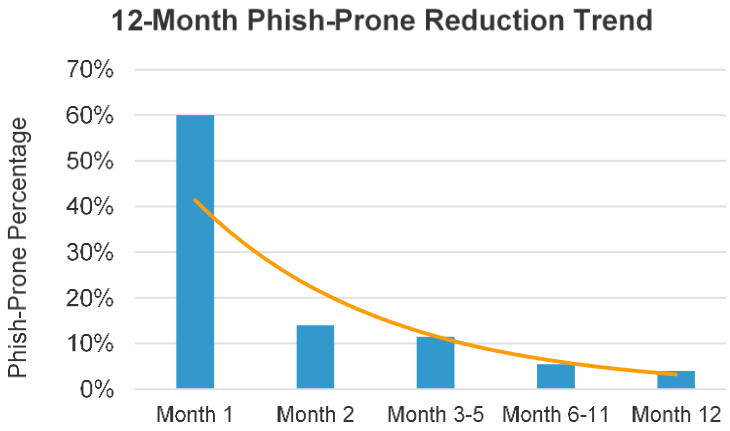
Results

The interview revealed the following themes:

- **To achieve desired results, the CISO demanded leadership support and buy-in.** The CISO convinced the organization's leadership to agree to phishing simulations that leverage spoofing and a cycle built around lessons and simulation. When the customer ran its first phishing simulation with KnowBe4, it received a 60% phish-prone percentage; that is, 60% of all staff clicked on a link that could have been harmful to the organization or somehow compromised data or access. Given transparency and proper training content and regimens after the first simulation, the organization's phish-prone percentage fell to 14% the next month. Leaders were especially surprised, as the phishing content for the second test was related to a recent major sports championship victory by the local professional sports team and the email promised memorabilia. In one month, leadership observed the power of having proper security awareness training and giving staff notice about simulated phishing attacks. This led to an acute vigilance that built the foundation for this organization's human firewall. Furthermore, the organization was able to further test the effectiveness by customizing and tailoring each attack based on relevant events and analyzing which templates work best given time and audience. The customer found its phish-prone percentage dropping to 11% to 12% in months 3 to 5, stabilizing at 5% to 6%, and reaching 4% near the one-year mark after adopting KnowBe4, as illustrated in Figure 3.

FIGURE 3

12-Month Phish-Prone Reduction Trend



Source: Forrester Research, Inc.

- **Incentivizing behavior change and aligning individual staff performance reinforces your human firewall.** The customer estimates about 1.5 million emails are delivered, while 23 million are blocked each month. Over 200,000 of these emails are known to have malware and 19,000 have a targeted attack attachment. The customer understood that there will be gaps that the security hardware and software cannot fill quickly enough and that the people need to be part of the line of defense. The customer highlighted it was pleasantly surprised with how well the Phish Alert button has worked. Staff are encouraged to submit Phish Alerts, and they will be rewarded with "points" when they correctly identify a monthly phishing test email. These points funnel directly into the performance management system and play a material role in the staff's performance reviews each year. The program was so successful that the IT security team not only found additional threats and gaps to beware of based on the employee-supplied intelligence, but the team also found certain legitimate messages that did not pass the eye test and users assumed were phishing emails. In these cases, the security team worked with the

senders to properly announce the email and reformat the email in a way to reduce the potential of it being reported as a phishing email. For users who continued to fail the testing each month, additional KnowBe4 training modules were assigned to reinforce the key areas of identifying phishing emails. Readers should note that building a human firewall may take time and the right mix of incentives to incite behavior changes. This customer example answers very well to Forrester's application of behavioral principles to security awareness, which readers may use as reference, as shown in Figure 4.[8]

FIGURE 4

An Example Of Behavioral Principles Applied To Security Awareness

Behavioral attribute	Components	Example
Motivation	Potential consequences , to both organization and self, of noncompliance	Do staff members realize the damage that malware can do to the firm and the implications for their role?
	Expectations implied by organizational culture	Does the firm encourage a "speak up" and "safety first" culture?
	Current state , or mood, of the individual	Are users too stressed, busy, or focused on other things to remain motivated?
Ability	Awareness of expected behavior	Are staff members aware that links within emails can be malicious?
	Simplicity of expected behavior	• How simple is it to spot a potentially malicious link in email? • How disruptive will it be to not immediately click on the link?
Trigger	Immediacy or "actionability"	• What prompts are available to individuals as they open the email? • If staff members spot a potentially malicious email, how many steps do they have to go through to take the expected action?

Source: Forrester Research, Inc.

BENEFITS

The interviewed organization experienced three benefits in this case study:

- Mitigating risk of revenue loss, reputation loss, and increased cost of compliance.
- Reduction in breach remediation costs.
- Third-party simulation cost avoidance.

Mitigating Risk Of Revenue Loss, Reputation Loss, And Increased Cost Of Compliance

As the customer had not experienced any material breaches, this portion of the model is conceptually presented for readers. It incorporates all areas that the customer and Forrester consider important when building a business case to invest in a risk mitigation solution typically related to corporate security.

This conceptual model contains three main components. The first component relates to revenue loss. Readers can divide annual revenue by either workable or total hours in each year. The revenue per hour can then be multiplied against the estimated downtime due to social engineering breaches.

The second component relates to decreased customer retention, increased attrition, or reduced lifetime value due to reputation loss from publicized breaches. The average value per customer can be multiplied by departing customers based on the estimated attrition rate.

The third component is a sum of all the incremental "external" expenses resulting from breaches. An internal expense is related to issue resolution and remediation like workstation reimaging or server recovery. External expenses are dollars that are an outflow from the organization. This includes items like fines, penalties, professional audit fees, and any other investments in compliance or controls.

Adding the estimated total from each of the three components will give users an idea of the value of risk mitigation. The risk adjustment for conceptual areas can typically run a bit higher, at 20%, especially if the customer is unsure of the probability of success by deploying KnowBe4. Readers are encouraged to begin developing business cases as they engage KnowBe4 and revise the case during or after a trial or proof of concept (POC).

TABLE 1
Cost And Utilization Optimization

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
Z1	Annual revenue	User estimate				
Z2	Revenue per hour	Z1/2,080 or Z1/8,760				
Z3	Downtime due to social engineering breaches	User estimate				
Z4	Potential revenue loss	Z2*Z3				
Z5	Total customers	User estimate				
Z6	Average value per customer	Z1/Z5				

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
Z7	Reduction in renewals/increase in attrition (churn) due to social engineering breaches	User estimate				
Z8	Potential reputation loss	Z5*Z7*Z6				
Z9	Fines and penalties due to breach	User estimate				
Z10	Professional and audit fees incurred	User estimate				
Z11	Incremental compliance and controls investments	User estimate				
Z12	Potential increase in cost of compliance	Z9+Z10+Z11				
Zt	Value of risk mitigation	Z4+Z8+Z12				
	Risk adjustment	↓20%				
Ztr	**Value of risk mitigation (risk-adjusted)**	**Zt*risk adjustment**	**$0**	**$0**	**$0**	**$0**

Source: Forrester Research, Inc.

Reduction In Breach Remediation Costs

Prior to deploying KnowBe4, the customer estimated an average of 20 workstations reimaged and two servers recovered each month. Each workstation reimaging takes 1 hour of IT staff time and non-IT staff time, whereas server recoveries take two days. This estimate essentially fits into a typical “many small” and “few larger” breakout of issues. This customer estimated a 1 to 10 ratio for large to small issues. Readers may want to determine a similar and fitting ratio for their organizations and plug in both the volume of issues and resolution times. It is vital to consider both the IT staff time needed for remediation and the nonproductive time for non-IT staff if they are not able to work.

Over three years, the customer experienced a $124,219 benefit value after adjusting for risk, as shown in Table 2.

TABLE 2
Reduction In Breach Remediation Costs

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
A1	IT security resource salary	Year 1: assumption Years 2 and 3: $A1_{py}$*103%		$120,000	$123,600	$127,308
A2	Non-IT security resource salary	Year 1: assumption Year 2 and 3: $A2_{py}$*103%		$75,000	$77,250	$79,568
A3	Pre-KnowBe4 workstation reimaging events per month	Customer estimate		20	20	20
A4	Pre-KnowBe4 server recovery events per month	A3*10%		2	2	2
A5	Resolution hours per workstation reimaging issue	Customer estimate		1	1	1
A6	Resolution hours per server recovery issue	Customer estimate		16	16	16
A7	Total issue resolution time due to malware originating from phishing attack	((A3*A5)+(A4*A6))*12		624	624	624
A8	IT security cost avoidance	(A1/2,080)*A7		$36,000	$37,080	$38,192
A9	Non-IT security productivity	(A2/2,080)*(A3*A5*12)		$8,654	$8,913	$9,181
At	Reduction in breach remediation costs	A8+A9		$44,654	$45,993	$47,373
	Risk adjustment	↓10%				
Atr	**Reduction in breach remediation costs (risk-adjusted)**		**$0**	**$40,188**	**$41,394**	**$42,636**

Source: Forrester Research, Inc.

Third-Party Simulation Cost Avoidance

This benefit category allows the customer to compare the cost effectiveness of KnowBe4 with the closest alternative. The customer estimated that the monthly cost of a third-party company to conduct phishing simulations would be similar to KnowBe4's annual cost. To conservatively and realistically adjust, these third-party companies may function similar to an MSSP and provide more services than just phishing simulation. Also, under this cost configuration and lower level of control and customization, the customer may run tests at a quarterly interval instead of monthly.

Thus, the model accounts for 50% of the monthly third-party cost and schedules quarterly phishing simulations. Over three years, the customer experienced a $375,000 benefit value after adjusting for risk, as shown in Table 3. Readers should note that they may insert their closest alternative in this part of the model regardless of

whether they are using a third party or internally building a simulator and training content. It is important to note any enhancements or deficiencies between the closest alternative and KnowBe4 to adjust for a "like-to-like" comparison of cost and function.

TABLE 3
Third-Party Simulation Cost Avoidance

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
B1	KnowBe4 annual cost	Customer estimate		$62,500	$62,500	$62,500
B2	Third-party simulations per year	Assumption		4	4	4
Bt	Third-party simulation cost avoidance	B1*B2		$250,000	$250,000	$250,000
	Risk adjustment	↓50%				
Btr	**Third-party simulation cost avoidance (risk-adjusted)**		**$0**	**$125,000**	**$125,000**	**$125,000**

Source: Forrester Research, Inc.

Total Benefits

Table 4 shows the total of all benefits across the two quantified areas listed above, as well as present values (PVs) discounted at 10%. Over three years, the interviewed customer expects risk-adjusted total benefits to be a PV of $413,634.

TABLE 4
Total Benefits (Risk-Adjusted)

Ref.	Benefit Category	Initial	Year 1	Year 2	Year 3	Total	Present Value
Atr	Reduction in breach remediation costs	$0	$40,188	$41,394	$42,636	$124,219	$102,778
Btr	Third-party simulation cost avoidance	$0	$125,000	$125,000	$125,000	$375,000	$310,856
	Total benefits (risk-adjusted)	**$0**	**$165,188**	**$166,394**	**$167,636**	**$499,219**	**$413,634**

Source: Forrester Research, Inc.

COSTS

The interviewed organization experienced two primary costs associated with the solution:

- KnowBe4 solution cost.
- Internal labor and implementation.

KnowBe4 Solution Cost

This cost accounts for the total solution cost based on per-user licensing; total licenses; and packaging, services, or features included. As pricing may range based on the quantity of users and packaging, readers are encouraged to reach out to KnowBe4 for a tailored quote to enter in their business case and model.

Internal Labor And Implementation

This cost incorporates 6 hours each month dedicated to ongoing operations for phishing simulation and security awareness training. The customer highlighted that 3 to 4 hours are spent consuming the analytics, selecting and customizing the phishing templates, and targeting specific groups as relevant. The customer adds that it spends an hour to reconcile new and retired user accounts and another hour to load performance management data related to earned points for Phish Alerts.

Total Costs

Table 5 shows the total of all costs as well as associated PVs, discounted at 10%. Over three years, the interviewed organization expects total costs to be a PV of $182,125.

TABLE 5
Total Costs (Risk-Adjusted)

Ref.	Cost Category	Initial	Year 1	Year 2	Year 3	Total	Present Value
Ctr	KnowBe4 solution cost	$0	$68,750	$68,750	$68,750	$206,250	$170,971
Dtr	Internal labor and implementation	$0	$4,362	$4,492	$4,627	$13,481	$11,154
	Total costs (risk-adjusted)	**$0**	**$73,112**	**$73,242**	**$73,377**	**$219,731**	**$182,125**

Source: Forrester Research, Inc.

FLEXIBILITY

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

The customer highlighted three areas that the IT security team will explore going forward. The first is to continue leveraging new phishing templates and release new training videos to the organization's users. Although the phish-prone percentage was largely in the single digits for the past year, there have been pockets or departments that were particularly susceptible to phishing. One such instance included spoofing the group's director and saw a 70% click-through rate (CTR) for that particular simulation. Instead of running the same tests to stabilize results for optics' sake, the organization will continue to target differently, customize templates based on current and relevant events, and increase difficulty as necessary to continually improve the organization's readiness.

The organization may also begin looking at phishing simulations beyond email. KnowBe4 offers tests that range from phone phishing (vishing) to SMS phishing (smishing) to physical penetration testing via "unknown" USB drives. For organizations that may have espionage in their threat models, this expanded set of social engineering penetration tests becomes more relevant and important to include.[9]

Lastly, the organization will also work with KnowBe4 to create a quicker and more efficient method to reconcile new and retired user accounts. This will both reduce the extra hour of effort each month and set up the organization to more easily include nonemployee user accounts like contractors and students.

RISKS

Forrester defines two types of risk associated with this analysis: "implementation risk" and "impact risk." Implementation risk is the risk that a proposed investment in KnowBe4 may deviate from the original or expected requirements, resulting in higher costs than anticipated. Impact risk refers to the risk that the business or technology needs of the organization may not be met by the investment in KnowBe4, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for cost and benefit estimates.

TABLE 6
Benefit And Cost Risk Adjustments

Benefits	Adjustment
Reduction in breach remediation costs	↓ 10%
Third-party simulation cost avoidance	↓ 50%
Costs	**Adjustment**
KnowBe4 solution cost	↑ 10%
Internal labor and implementation	↑ 5%

Source: Forrester Research, Inc.

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

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

- Lack of training and reinforcement to coincide with simulations.
- Failure to incentivize and incite behavior change to create a human firewall.
- An unengaged IT security team that runs the same test for the same groups each month without adjusting for difficulty or relevance.
- Overlapping and redundant processes, tools, and security providers.

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

- Increased user or service footprint.
- Preference to further customize training materials.

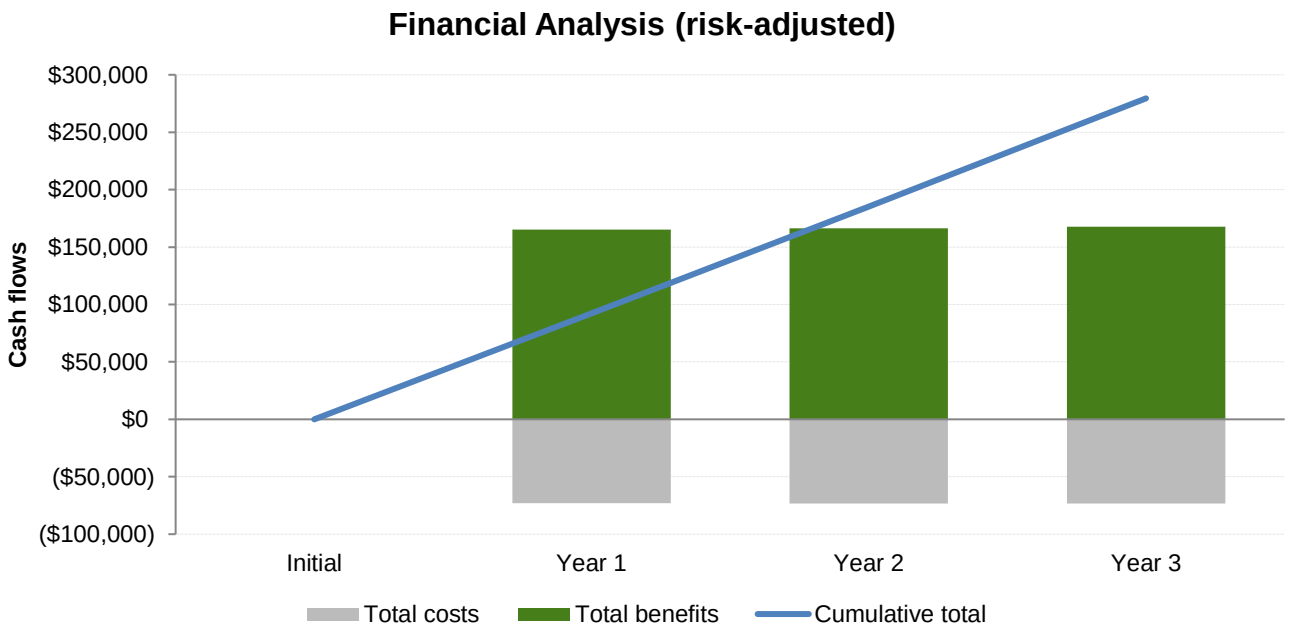
Table 6 shows the values used to adjust for risk and uncertainty in the cost and benefit estimates for the interviewed organization. Readers are urged to apply their own risk ranges based on their own degree of confidence in the cost and benefit estimates.

Financial Summary

The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the interviewed organization's investment in KnowBe4.

Table 7 below shows the risk-adjusted ROI, NPV, and payback period values. These values are determined by applying the risk-adjustment values from Table 6 in the Risks section to the unadjusted results in each relevant cost and benefit section.

FIGURE 5
Cash Flow Chart (Risk-Adjusted)



Source: Forrester Research, Inc.

TABLE 7
Cash Flow (Risk-Adjusted)

Summary	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	$0	($73,112)	($73,242)	($73,377)	($219,731)	($182,125)
Total benefits	$0	$165,188	$166,394	$167,636	$499,219	$413,634
Total	**$0**	**$92,077**	**$93,152**	**$94,259**	**$279,487**	**$231,509**
ROI			**127%**			
Payback period (months)			**< 1 month**			

Source: Forrester Research, Inc.

KnowBe4: Overview

The following information is provided by KnowBe4. Forrester has not validated any claims and does not endorse KnowBe4 or its offerings.

KnowBe4's Enterprise Awareness Training Program provides a comprehensive “new-school” approach that integrates baseline testing using mock attacks, engaging interactive web-based training, and continuous assessment through simulated phishing, vishing, and smishing attacks to build a more resilient and secure organization.

Solution highlights include:

- **An integrated platform.** KnowBe4’s platform integrates all functions into a single, user-friendly GUI. Training campaigns and simulated attacks can be initiated in minutes. Customers can completely customize templates, landing pages, and simulated attachments, and even spoof their own domain for simulated CEO fraud attacks.
- **Random attack delivery.** KnowBe4 provides customers with "double-random" message delivery. Choose from hundreds of highly realistic phishing messages, spread over time. Every employee receives a different phishing email at a different time. New templates from the wild are constantly added, and KnowBe4 creates "Current Events" templates for you.
- **Unlimited use.** A subscription provides unlimited access to all features, modules, and assessments with flexible licensing. There are no artificial license ceilings, true-up once a year. New features are added regularly, and the platform is multilingual in nine languages.
- **Superior tech support.** As an enterprise customer, organizations are automatically enrolled in the Platinum Tech Support program. KnowBe4 is US-based and provides short response times with a referenceable reputation.
- **Managed services.** KnowBe4 has experts who will work with customers to create a project that meets the organization’s unique needs and provide actionable reports to improve end user security. The managed services option is fully customizable.
- **Improved security behavior.** Referenceable customers have shown that the KnowBe4 approach works. Repeated studies show that the employee phish-prone percentage drops more than 90%. The free Phish Alert button email reporting add-in reinforces security training.
- **Security awareness training content.** An extensive library of security awareness training content includes interactive modules, videos, games, posters, and newsletters.

Appendix A: Interviewed Customer Description

For this study, Forrester interviewed a large, US-based healthcare network with the following characteristics:

- Comprises 10 medical facilities.
- Has over 10,000 user accounts, with 1,000 to 2,000 reserved for nonemployees such as students and contractors.
- Has a IT security team of 16 people with a budget of more than $4 million.

INTERVIEW HIGHLIGHTS

The interviewed customer highlighted the following pre-KnowBe4 issues and gaps, technology selection criteria and goals, and post-KnowBe4 deployment results.

Situation

Prior to engaging KnowBe4, the interviewed customer did not conduct phishing simulations and provided the bare essentials for annual security awareness training. There was not a lot of proactive or interactive follow-up to the once-a-year compliance training. Articles or alerts that were sent or posted on the intranet were typically reactive to security events in the news. After onboarding a new director to lead information security, the organization built out its security infrastructure and processes. Eight years later, the team had established technical controls and processes and realized that end users were the remaining weak link. The organization sought to reduce its vulnerability to social engineering threats.

Solution

The interviewed customer reviewed several options, including developing an internal awareness training and phishing simulator, employing a third party to conduct phishing tests, and adopting a platform that would allow the IT security team to plan and customize phishing simulations. The customer ultimately selected KnowBe4 based on the following criteria:

- An intuitive user interface with minimal training needed.
- Customizable phishing templates and targeting.
- Accessibility and completeness of training content.
- Cost effectiveness relative to options considered.

After selecting KnowBe4, the interviewed customer deployed with the following goals, which were achieved in Year 1:

- Reduce the phish-prone percentage from 60% in diagnostic tests to single-digit percentages in one year.[10]
- Continually increase simulation effectiveness by tailoring phishing content to current events, spoofing domains and people, and targeting specific groups.
- Leverage the Phish Alert button to build toward a “human firewall.”
- Build security awareness and proactive alerting into the organization’s performance management and incentives system.

FRAMEWORK ASSUMPTIONS

Table 8 provides the model assumptions that Forrester used in this analysis.

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

TABLE 8
Model Assumptions

Ref.	Metric	Value
X1	Hours per week	40
X2	Weeks per year	52
X3	Hours per year (M-F, 9-5)	2,080
X4	Hours per year (24x7)	8,760
X5	IT security resource annual salary	$120,000
X6	Non-IT security resource annual salary	$75,000
PY	Previous year	

Source: Forrester Research, Inc.

Appendix B: Total Economic Impact™ Overview

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

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

BENEFITS

Benefits represent the value delivered to the user organization — IT and/or business units — by the proposed product or project. Often, product or project justification exercises focus just on IT cost and cost reduction, leaving little room to analyze the effect of the technology on the entire organization. The TEI methodology and the resulting financial model place equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization. Calculation of benefit estimates involves a clear dialogue with the user organization to understand the specific value that is created. In addition, Forrester also requires that there be a clear line of accountability established between the measurement and justification of benefit estimates after the project has been completed. This ensures that benefit estimates tie back directly to the bottom line.

COSTS

Costs represent the investment necessary to capture the value, or benefits, of the proposed project. IT or the business units may incur costs in the form of fully burdened labor, subcontractors, or materials. Costs consider all the investments and expenses necessary to deliver the proposed value. In addition, the cost category within TEI captures any incremental costs over the existing environment for ongoing costs associated with the solution. All costs must be tied to the benefits that are created.

FLEXIBILITY

Within the TEI methodology, direct benefits represent one part of the investment value. While direct benefits can typically be the primary way to justify a project, Forrester believes that organizations should be able to measure the strategic value of an investment. Flexibility represents the value that can be obtained for some future additional investment building on top of the initial investment already made. For instance, an investment in an enterprisewide upgrade of an office productivity suite can potentially increase standardization (to increase efficiency) and reduce licensing costs. However, an embedded collaboration feature may translate to greater worker productivity if activated. The collaboration can only be used with additional investment in training at some future point. However, having the ability to capture that benefit has a PV that can be estimated. The flexibility component of TEI captures that value.

RISKS

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

Appendix C: Glossary

Discount rate: The interest rate used in cash flow analysis to take into account the time value of money. Companies set their own discount rate based on their business and investment environment. Forrester assumes a yearly discount rate of 10% for this analysis. Organizations typically use discount rates between 8% and 16% based on their current environment. Readers are urged to consult their respective organizations to determine the most appropriate discount rate to use in their own environment.

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

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

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

Return on investment (ROI): A measure of a project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits minus costs) by costs.

A NOTE ON CASH FLOW TABLES

The following is a note on the cash flow tables used in this study (see the example table below). The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1. Those costs are not discounted. All other cash flows in years 1 through 3 are discounted using the discount rate (shown in the Framework Assumptions section) at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations are not calculated until the summary tables are the sum of the initial investment and the discounted cash flows in each year.

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

TABLE [EXAMPLE]
Example Table

Ref.	Metric	Calculation	Year 1	Year 2	Year 3

Source: Forrester Research, Inc.

Appendix D: Endnotes

[1] Source: “2016 Data Breach Investigations Report.” Verizon, April 2016 (http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf).

[2] Source: “Ransomware: How Consumers And Businesses Value Their Data,” IBM Security X-Force Research, December 2016 (https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03135USEN).

[3] Source: “Understand The State Of Data Security And Privacy: 2016 To 2017,” Forrester Research, Inc., December 7, 2016.

[4] Forrester risk-adjusts the summary financial metrics to take into account the potential uncertainty of the cost and benefit estimates. For more information, see the section on Risks.

[5] While Forrester TEI seeks to provide visibility and a fully tailorable model for readers, some portions of the model may be conceptual and not include prepopulated figures, as the interviewed customer does not have experience in certain benefit categories. Since the interviewed customer has not experienced a material loss of revenue, loss of reputation, or increased cost of compliance, this benefit category will be presented as a conceptual model without specific figures that factor into the study’s summarized metrics (i.e., ROI, NPV, and payback period). Although Forrester wants to remain independent and model based on reality, readers should note that assumptions and extrapolation may be needed when building business cases for risk mitigation solutions.

[6] Source: Kristi L. Stathis, “Ocean Tomo Releases 2015 Annual Study of Intangible Asset Market Value,” Ocean Tomo, March 5, 2015 (http://www.oceantomo.com/blog/2015/03-05-ocean-tomo-2015-intangible-asset-market-value/).

[7] “Phish-prone percentage” is a term coined by KnowBe4 and essentially extrapolates the click-through rate (CTR) of a phishing email sent to an organization.

[8] Source: “Reinvent Security Awareness To Engage The Human Firewall,” Forrester Research, Inc., December 17, 2014.

[9] Source: “Reinvent Your Penetration Tests In The Age Of Targeted Attacks,” Forrester Research, Inc., January 21, 2016.

[10] “Phish-prone percentage” is a term coined by KnowBe4 and essentially extrapolates the click-through rate (CTR) of a phishing email sent to an organization.