A Forrester Total Economic Impact™
Study Commissioned By HackerOne
May 2019

The Total Economic Impact™ Of HackerOne Challenge

Improved Security And Compliance

FORRESTER®

Table Of Contents

Project Director:
Jonathan Lipsitz

Project Contributor:
Jon Erickson

FORRESTER®

Key Benefits

Reduction in penetration testing duration:

50%

Total cost of ownership (TCO) savings per penetration test:

$41,350

Reduction in internal pen testing effort:

66%

Executive Summary

HackerOne provides security and compliance penetration (pen) testing services that help its customers identify and remediate real-world security vulnerabilities. HackerOne commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by utilizing its Challenge service. This is a one-time engagement (repeatable as desired) in which ethical hackers test designated systems and applications for vulnerabilities. HackerOne also provides report analysis, a.k.a. triage services, and remediation recommendations as part of the offering. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of a HackerOne Challenge on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four customers with experience using HackerOne Challenge. Prior to using HackerOne, the customers performed traditional pen testing to look for vulnerabilities and meet compliance requirements. However, these missed many vulnerabilities, including critical ones, and were mainly a “check-the-box” activity.

Key Findings

Quantified benefits. The following risk-adjusted present value (PV) quantified benefits are representative of those experienced by the companies interviewed:

- **The cost of HackerOne Challenge replaced traditional penetration testing costs.** Organizations eliminated the cost of previous traditional pen testing by switching to HackerOne. The total cost varied widely across interviewees. Some said that the eliminated costs were orders of magnitude higher than the HackerOne cost. Others said that they were spending more money with HackerOne to have more robust testing across multiple environments. In all cases, the time taken to complete pen testing and get the results significantly decreased, resulting in less internal effort. For the financial analysis, Forrester assumes that the cost of traditional pen testing was equal to the cost of one HackerOne Challenge with the optional Compliance add-on and that the internal effort had been 0.75 of an FTE for two months during each Challenge (this was replaced by lower internal costs, which are discussed in the Analysis Of Costs section of the study). The total eliminated costs were $156,784.
- **HackerOne Challenge reduced internal security and application development efforts.** Interviewees avoided hiring additional security experts because of the robustness of testing and remediation information on vulnerabilities being provided by HackerOne. They also said that better bug identification and knowledge transfer reduced application development time. For the financial analysis, one security analyst was not added, and 10 developers saved four days of development time related to two Challenges per year. This totaled $384,793 over three years.

Unquantified benefits. The interviewed organizations experienced the following unquantified benefits, which they said were more valuable than the monetary savings:

ROI
115%

Benefits PV
$541,577

NPV
$289,450

Payback
< 6 months

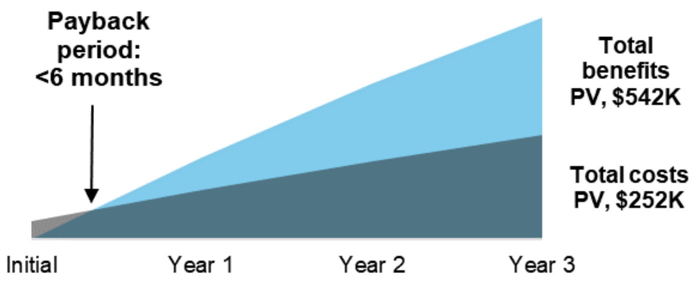
- **Security greatly improved, reducing the likelihood of a security breach.** All interviewees said that the quality of pen testing performed by HackerOne was much better than before because of the HackerOne methodology using ethical hackers with a wide range of skills and experiences. Interviewees also said that they received findings and recommendations faster, which allowed for an iterative remediation process unlike the traditional pen test findings, which were delivered all at once and usually too late to actively remediate before release. Altogether, this reduced the risk of a breach, which could be catastrophic in terms of cost and reputation. Improved testing also made for better audits by providing better documentation. A 2018 Ponemon Institute study estimated that the average worldwide cost of a breach was $3.86 million, and the likelihood of a breach in any given year was 13.95%.[1] If a HackerOne Challenge found the vulnerability before it was exploited, that could result in an additional $538,470 savings for each incident. That would increase the ROI to 646% and the NPV to $1.6 million.
- **Moving to HackerOne Challenge increased customer satisfaction and retention.** Interviewees reported that having more robust audits made existing customers more confident in their companies' ability to securely provide the contracted services. It also prevented customers from leaving because of security flaws or delayed audit results.

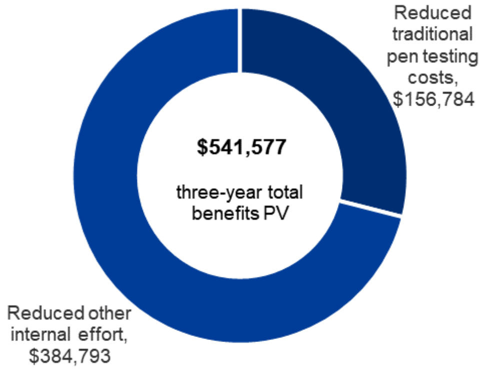
Costs. The interviewed organizations experienced the following risk-adjusted PV costs:

- **Two HackerOne Challenges were completed each year.** Both the development and production systems were tested once per year using HackerOne Challenge with the optional Compliance add-on. Previously, only the production system was tested once per year as more of a "check-the-box" compliance activity. The total cost over the life of the study was $216,845.
- **HackerOne Challenge required internal effort, though this effort was less than with previous testing.** Just 0.5 of an FTE was responsible for coordinating internal effort during each one-month Challenge for a total of two months elapsed time per year. Forrester did not include remediation effort in this analysis since that was business as usual regardless of testing approach. The total cost was $35,282.

Forrester's interviews with four existing customers and subsequent financial analysis (including only the quantified benefits) found that an organization based on these interviewed organizations experienced benefits of $541,577 over three years versus costs of $252,127, adding up to a net present value (NPV) of $289,450 and an ROI of 115%.

Financial Summary





TEI Framework And Methodology

From the information provided in the interviews, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering utilizing HackerOne Challenge.

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 HackerOne Challenge can have on an organization:

The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

DUE DILIGENCE
Interviewed HackerOne stakeholders and Forrester analysts to gather data relative to Challenge services.

CUSTOMER INTERVIEWS
Interviewed four organizations using HackerOne Challenge to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION
Designed a composite organization based on characteristics of the interviewed organizations.

FINANCIAL MODEL FRAMEWORK
Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewed organizations.

CASE STUDY
Employed four fundamental elements of TEI in modeling HackerOne Challenge's impact: 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 A for additional information on the TEI methodology.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by HackerOne 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 HackerOne Challenge.

HackerOne 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.

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

The HackerOne Challenge Customer Journey

BEFORE AND AFTER THE HACKERONE CHALLENGE INVESTMENT

Interviewed Organizations

For this study, Forrester conducted four interviews with HackerOne Challenge customers. Interviewed customers include the following:

INDUSTRY	INTERVIEWEE	CHALLENGE FOCUSES
Government	• Program manager • Digital services expert	• Public websites and web applications • Internal systems
Data analytics	• Chief security officer (CSO)	• PCI DSS and FedRamp compliance • Development and production environments
Web-based marketing	• Director	• SaaS solutions • Development and production environments
Payment solutions	• Engineering director	• PCI DSS compliance • Production environment

Key Problems

Interviewees faced several key problems with previous pen testing:

- **Previous pen testing missed critical vulnerabilities.** Traditional pen testing was missing critical vulnerabilities and sometimes focusing on irrelevant vulnerabilities that would not occur in a real attack, e.g., needing physical access to a machine. This left systems vulnerable and risked breaches that could result in large remediations costs, lost customers and revenue, and reputational damage. One interviewee said: "[Pen testing] used to be a frustrating process. What they were finding wasn't relevant. For example, they said the password was being exposed in the computer's memory. What does it matter? If you broke in and got physical access to the computer, you could put in a keylogger. They weren't finding practical exploits."

- **An audit was often a "check-the-box" activity.** In many cases, the goal of the audit-related penetration testing was just to mark it as completed. It did not provide much value in actually improving security or creating a greater sense of confidence with customers. "We are in a highly regulated industry — PCI, GDPR, SOX, and so on. I was paying for quarterly compliance pen tests. They were 'checking the box.' I always wanted them to find something. After two years, they still didn't find anything. We are good, but not that good."

- **Creating an in-house bug bounty program would have been too labor-intensive.** Several companies looked at creating their own bug bounty programs but concluded that building out the systems and processes internally would have been too costly and time-prohibitive. "My predecessor had been thinking about using bug bounties. The prospect of doing it all on our own was daunting, especially when companies like HackerOne offer this service."

"The pen tests used to be limited by the skill level of the assigned team. Sometimes they get very settled in how they approached a problem. When you bring in the crowd with HackerOne, you have different perspectives and better results."

Program manager, government

"[Former pen test engagements] felt like they were just trying to check the box. They would run a piece of software without taking the time to understand how the target system works. With HackerOne, they take the time to understand the systems and really try to get in."

Engineering director, payment solutions

Key Results

The interviews revealed several key results from the HackerOne Challenge investment:

- **HackerOne found more vulnerabilities and provided better remediation recommendations.** The most important benefit was finding more vulnerabilities, both in terms of numbers and criticality, in order to remediate them and create better system security. This could be across internal- and external-facing systems, websites, mobile applications, and internet-of-things (IoT) devices. Better security delivers many benefits that are discussed throughout this study. “We had some vulnerabilities found in our first Challenge. We learned a lot from the triaging and created a remediation cycle for high and critical vulnerabilities.”
- **Compliance and audits improved.** Auditors accepted HackerOne Challenge’s testing methodologies and Security Assessment Reports for SOC2 Type 2, PCI DSS, and HITRUST certification. Interviewees’ customers welcomed better compliance and more meaningful audits. This often resulted in better customer retention and winning more customers. “Our audits are now a point of trust with prospects. HackerOne wound up being a revenue-generating opportunity.”
- **The effort to manage pen testing decreased.** HackerOne manages the pen testing process to reduce customers’ effort and provide results faster. One interviewee said: “Traditional pen tests can be very expensive and take months. You can get past a lot of that with HackerOne.”

Composite Organization

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an associated ROI analysis that illustrates the areas financially affected. The composite organization is representative of the four companies that Forrester interviewed and is used to present the aggregate financial analysis in the next section. The composite organization that Forrester synthesized from the customer interviews is a US-based software-as-a-service (SaaS) company with global operations. It holds PII and cardholder information. It completes two HackerOne Challenges per year for audited compliance certification (in addition to an ongoing engagement with HackerOne looking at other vulnerability areas, which is out of scope for this study). One test is on the production environment, which is required by its Qualified Security Assessor (QSA), and the other is on the development environment.

> “Bug bounties are, by design, ambiguous because you don’t know what you don’t know. Some of the most interesting vulnerabilities no machine or automated system could have found. Researchers will often work together, when invited, to tie together a bunch of small vulnerabilities that add up to a critical issue.”
>
> *Digital services expert, government*

> “We worked with our auditor to make sure they would be happy. HackerOne worked with us to add operations and networking sections to the summary report. That is now accepted by our auditors for compliance.”
>
> *Engineering director, payment solutions*

Key assumptions

SOC and PCI compliance requirements

Development and production pen testing

Analysis Of Benefits

QUANTIFIED BENEFIT DATA AS APPLIED TO THE COMPOSITE

Total Benefits

REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Reduced traditional pen testing costs	$63,045	$63,045	$63,045	$189,135	$156,784
Btr	Reduced other internal effort	$154,731	$154,731	$154,731	$464,193	$384,793
	Total benefits (risk-adjusted)	$217,776	$217,776	$217,776	$653,328	$541,577

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total benefits to be a PV of $541,577.

Reduced Traditional Pen Testing Costs

HackerOne Challenge costs can be offset, partially or wholly, by reduced cost for other pen testing service providers and internal effort. Interviewees represented a wide range of experiences, from eliminated costs being many times more than what was being paid to HackerOne to HackerOne being slightly more expensive. Notably, organizations can complete Challenges much faster than traditional pen testing, which saves cost and effort and improves remediation. All interviewees viewed the costs being paid to HackerOne for these Challenges as negligible compared to the benefits associated with improved security (discussed later in the study).

From the interviews, Forrester heard:

- "Previously we had scanners-as-a-service doing static and dynamic code scanning. It found some bugs but was 10x to 15x more expensive per bug found and didn't find everything."
- "The comparable work we did in the pilot would have cost six times more with our previous service provider, and they gave us much fewer findings."
- "HackerOne is a much better cost model than red-team pen testing. It is far cheaper to run bug bounties than to do traditional pen testing. And you get much better results."
- "Every $1 we spend on HackerOne Challenges would have meant $5 in the past for other pen testing and auditors."
- "We avoid the one to two months preplanning that was needed to make sure all system owners were onboard."
- "They take care of the triage, which saves my team time. HackerOne tries to recreate the bugs, which is very helpful. Sometimes hackers file a bug, which is just a misunderstanding."
- "HackerOne does so much of the overhead work. They provide the online submissions platform, manage the researchers, and provide industry best practices on structuring the programs and making payments. It eliminated the need to recreate the wheel."

For the financial analysis, Forrester assumes:

> "If you break it down as bounty payouts compared to the quality of vulnerabilities found and time saved, HackerOne is a much better ROI compared to traditional pen testing companies."
>
> *Digital services expert, government*

- To be conservative, the cost for a single pen test from the previous provider was the same for a HackerOne Challenge with optional Compliance add-on.
- The organization previously conducted only one pen test per year. Therefore, the savings shown here are equal to one of the two HackerOne Challenges shown in the Analysis Of Costs section of the study.
- Previous pen testing took two months and required 0.75 of an FTE to manage the testing internally and lead triaging efforts. (The HackerOne-related internal effort, which replaced this is shown in the Analysis Of Costs section of the study.)

The amount of cost and effort expended on previous testing can vary widely from greater to less than HackerOne based on the nature of the systems and information being tested and the high-profile status of a company. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $156,784.

Impact risk is the risk that the business or technology needs of the organization may not be met by the investment, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for benefit estimates.

Reduced Traditional Pen Testing Costs: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
A1	Third-party fees	Ctr/2	$36,300	$36,300	$36,300
A2	Internal effort	2 months*2 Challenges*.75 FTE*($135,000/12 months)	$33,750	$33,750	$33,750
At	Reduced traditional pen testing costs	A1+A2	$70,050	$70,050	$70,050
	Risk adjustment	↓10%			
Atr	Reduced traditional pen testing costs (risk-adjusted)		$63,045	$63,045	$63,045

Reduced Other Internal Effort

Using HackerOne Challenge improved other IT activities beyond the pen testing savings described above. Interviewees avoided hiring security analysts, reduced application development time, and upskilled their IT security teams. This was attributed to better and more timely information about vulnerabilities being shared with the IT team and developers. Additionally, the ability to interact with the researchers/hackers provided great learning opportunities for the IT organization and developers. Forrester heard from interviewees:

- “Onboarding new vendors as part of our solutions is a pain in terms of security testing. Now, whenever we bring on a new vendor, we make it part of our Challenge in the testing phase. That saves us time.”
- “We have seen a reduction in internal effort for developers. There is less rework, and they write better code. This is FTE savings that can be used for other activities.”
- “HackerOne scales with us. We ran a Challenge around a Super Bowl-related service and tested 1.2 petabytes of data.”
- “Conversations with the actual hackers to understand how and why they did things is priceless. We gave some of our developers access to the HackerOne portal so they could better understand what was done. This increases our internal skills.”

> “The fact that we have a contract with HackerOne means we don’t have to hire a security analyst right now.”
>
> *Engineering director, payment solutions*

- “Challenges open our developers’ eyes to what exploits can be accomplished. We will provide more security training based on this to avoid exploits in the first place and save time.”

Forrester assumes:

- The composite organization avoided hiring one security analyst because of the services and information provided by HackerOne.
- Ten developers each saved 4 hours of coding time after each Challenge as their skills improved and because of better vulnerability-related information being provided.

This benefit can vary based on the size of the IT security organization as well as the number and type of developers. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $384,793.

Reduced Other Internal Effort: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
B1	Avoided security analyst	1FTE*$135,000	$135,000	$135,000	$135,000
B2	Reduced application development	10 developers*4 days*2 Challenges*$461.54	$36,923	$36,923	$36,923
Bt	Reduced other internal effort	B1+B2	$171,923	$171,923	$171,923
	Risk adjustment	↓10%			
Btr	Reduced other internal effort (risk-adjusted)		$154,731	$154,731	$154,731

Unquantified Benefits

Improved Security And Audits

The most important benefit of using HackerOne Challenge was improved security. Every interviewee provided many examples of how their security has improved for both internal and external systems and applications. This meant a reduced likelihood of a breach occurring. The 2018 Ponemon Institute study estimated the following costs of a breach:[2]

> “Before, an external company would do a pen test and then report on it. We would then have to make fixes and run the test again. Now we have a state of continuous compliance. It has made audits more agile.”
>
> *CSO, data analytics*

- Average total cost of a data breach: $3.86 million.
- Likelihood of a breach in any one year: 13.95%.
- Average cost per lost or stolen record: $148.
- Meant-time-to-identify (MTTI): 197 days.
- Mean-time-to-contain (MTTC): 69 days.
- Likelihood of a recurring material breach over the next two years: 27.9%.

No cost savings from reduced likelihood and severity of a breach were included in the main ROI calculations because it will vary so widely from one company to the next. Readers are encouraged to think about the possible cost savings from fewer vulnerabilities. For example, applying the Ponemon Institute numbers could result in an additional savings of $538,470 per year ($3.86 million x 13.95%) if a HackerOne Challenge identified the vulnerability before being exploited. That would increase the study’s ROI and NPV from 115%/$289,450 to 646%/$1.6 million.

Interviewees provided the following examples of how their security and audits have improved:

- “A Challenge is a really good way to get an army of hackers to pound on systems and get results quickly. HackerOne gets us as many resources as we need.”
- “Speed was very impressive. Once the Challenge launched, we saw some really good things coming in. Everyone on our side cleared their calendars to fix the vulnerabilities.”
- “New hackers would test the same bugs and sometimes find new ways to break them after we had already fixed it. We would ask the hackers about their thought processes. In a traditional pen test model, we would have just assumed a vulnerability was fixed the first time. Now it is much more iterative.”
- “The biggest benefit is the nature of the hackers. They are skilled and motivated. They will actually find things. I don’t know why the previous pen testers did not.”
- “We found 138 vulnerabilities in our first Challenge. They were found much faster and of higher complexity than what we had gotten from past providers.”
- “Researchers found ways around some of our protections that we didn’t think they could. They didn’t play the game the way we expected.”
- “We do the Challenge and then bring the auditors in. We use compliance to make the platform more secure.”
- “They found an exploit that allowed them to read local files on the server. That was terrifying.”
- “We did work to prevent one particular exploit type, and these guys very cleverly ripped it apart.”
- “They found vulnerabilities that hadn’t been found before. It improves security and our overall quality.”

> “The cost of the program is insignificant compared to if we were hacked for real.”
>
> *Director, web-based marketing*

In addition to finding vulnerabilities, HackerOne provides very actionable information during the Challenge and in a summary report afterwards. Interviewees found this information very useful, saying:

- “We could see the reports as they came in, which was great. HackerOne would triage them to make sure they were valid and remove duplicates. They would also prioritize based on severity and business impacts.”
- “In a traditional model, we would get the report and then send questions back to the tester. Responses would be delayed and slow, and the information coming back wasn’t concrete. HackerOne provided information [in] near real time, which was fantastic. By getting better information about complex, multistage vulnerabilities, we could fix related vulnerabilities too.”

Increased Customer Satisfaction And Retention

Even if a vulnerability would have never been exploited, customers are happier knowing that their information is safe. Interviewees reported that HackerOne Challenge made their customers (both internal and external) more confident in the security and services being provided. This resulted in better customer retention and even contributed to winning new customers. Interviewees said:

- “Advertising that we are in partnership with HackerOne helps with sales and marketing.”
- “Better compliance is the crown jewel. That is how you establish trust with people.”
- “When a PCI audit is delayed, companies don’t want to work with you. That can cost you business. Before starting the Challenges, that happened and lost us new business. It hasn’t happened since.”
- “Building trust with customers when everything is in the cloud is difficult and important. HackerOne helps with that.”

> “Trust is a very big factor because we handle customers’ operations. Challenges increase the trust level of our customers.”
>
> *Engineering director, payment solutions*

Flexibility

The value of flexibility is clearly unique to each customer, and the measure of its value varies from organization to organization. There are multiple scenarios in which a customer might choose to implement HackerOne Challenge and later realize additional uses and benefits. Some examples from interviewees included:

- Expanding testing to include IoT hardware.
- Including additional systems, e.g., internal systems and mobile apps.
- Testing on other public cloud providers.
- Moving to continual testing instead of serial Challenges.
- Training services from HackerOne.

Forrester did not include any of these future opportunities in the financial analysis.

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for a 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.

Analysis Of Costs

QUANTIFIED COST DATA AS APPLIED TO THE COMPOSITE

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Ctr	HackerOne Challenge fees	$36,300	$72,600	$72,600	$72,600	$254,100	$216,845
Dtr	Internal effort	$5,906	$11,813	$11,813	$11,813	$41,344	$35,282
	Total costs (risk-adjusted)	$42,206	$84,413	$84,413	$84,413	$295,444	$252,127

HackerOne Challenge Fees

HackerOne has several versions of its Challenge service (see the HackerOne Challenge: Overview section of the study). The composite organization used the HackerOne Challenge with optional Compliance add-on. The organization completed one Challenge as a pilot in the initial period and then two Challenges per year. The total list price for this type of Challenge is $33,000, which includes the HackerOne platform and report analysis services, a.k.a. triage, as well as the bug bounty pool. The pool may be expanded at the customer's discretion if there are many bugs being found.

The Challenge fees paid to HackerOne can vary based on the number and type of Challenges as well as the bug bounty pool size. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year risk-adjusted total PV of $216,845.

The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total costs to be a PV of $252,127.

Implementation risk is the risk that a proposed investment may deviate from the original or expected requirements, resulting in higher costs than anticipated. The greater the uncertainty, the wider the potential range of outcomes for cost estimates.

HackerOne Challenge Fees: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
C1	Number of Challenges		1	2	2	2
C2	Average cost per Challenge		$33,000	$33,000	$33,000	$33,000
Ct	HackerOne Challenge fees	C1*C2	$33,000	$66,000	$66,000	$66,000
	Risk adjustment	↑10%				
Ctr	HackerOne Challenge fees (risk-adjusted)		$36,300	$72,600	$72,600	$72,600

Internal Effort

As discussed in the Analysis Of Benefits section, the amount of internal effort to manage a Challenge is less than with traditional pen testing. Forrester included 0.5 FTEs to manage the processes from the company side in terms of working with HackerOne on triage, disseminating information, and coordinating communication with the hackers. Forrester excluded the effort to remediate vulnerabilities since this would be required regardless of the type of penetration testing taking place.

The internal effort may be higher depending on the scope of the Challenge and the number of vulnerabilities identified. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year risk-adjusted total PV of $35,282.

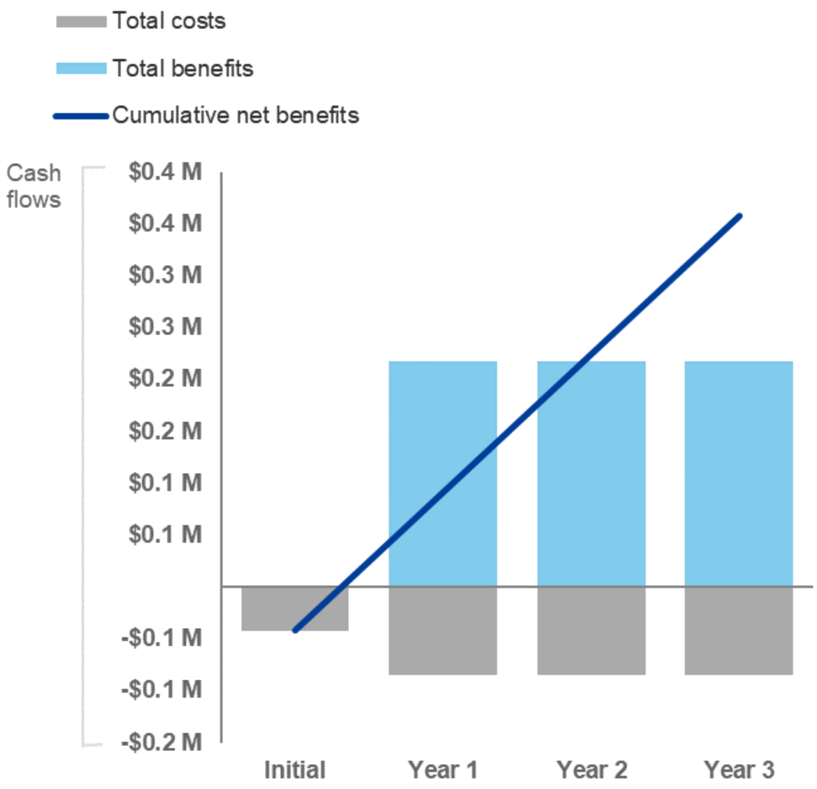
Internal Effort: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
D1	Number of months	C1*1 month	1	2	2	2
D2	Number of FTEs		0.5	0.5	0.5	0.5
D3	IT security fully burdened salary	$135,000/12 months	$11,250	$11,250	$11,250	$11,250
Dt	Internal effort	D1*D2*D3	$5,625	$11,250	$11,250	$11,250
	Risk adjustment	↑5%				
Dtr	Internal effort (risk-adjusted)		$5,906	$11,813	$11,813	$11,813

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 Table (Risk-Adjusted)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($42,206)	($84,413)	($84,413)	($84,413)	($295,444)	($252,127)
Total benefits	$0	$217,776	$217,776	$217,776	$653,328	$541,577
Net benefits	($42,206)	$133,363	$133,363	$133,363	$357,884	$289,450
ROI						115%
Payback period						<6 months

HackerOne Challenge: Overview

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

HackerOne Challenge reduces your risk of security incidents though private, time-bound, hacker-powered security tests all managed by an expert team:

- On-demand engagements of 15 to 180 days of active testing by the world’s largest, most diverse community of security talent.
- Includes setting the scope, inviting and working with hackers, submitted report analysis, and awarding bounties for validated reports.
- Includes optional access to HackerOne Clear network of background-checked and ID-verified hackers, HackerOne Clear VPN, and custom click-through hacker agreements.
- Includes optional capabilities for meeting the specific penetration testing requirements for compliance certifications, such as PCI DSS, SOC2 Type 2, and HITRUST.

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 A: Endnotes

[1] Source: “2018 Cost of a Data Breach Study: Global Overview,” Ponemon Institute, LLC, July 2018.
[2] Source: Ibid.