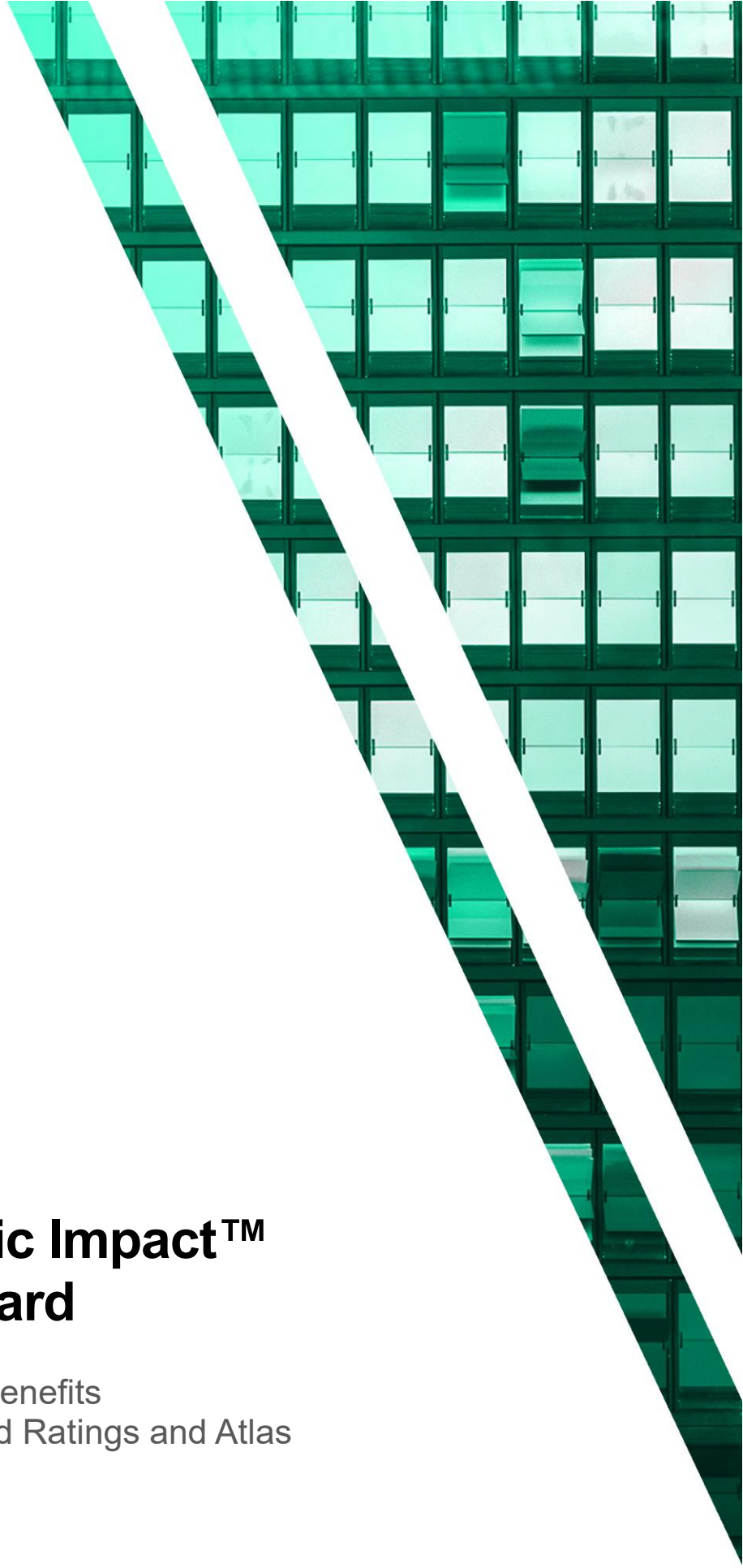
FORRESTER®



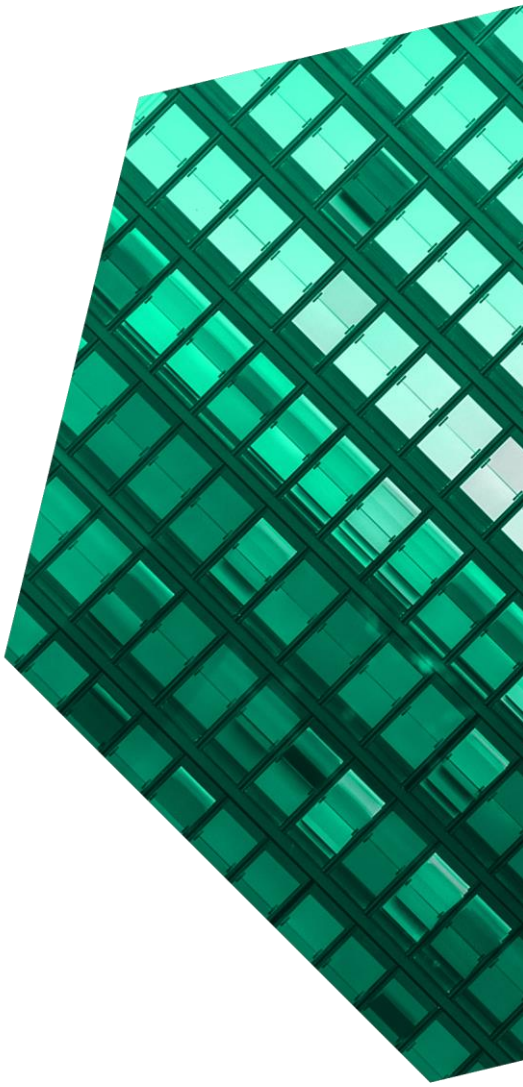
The Total Economic Impact™ Of SecurityScorecard

Cost Savings And Business Benefits Enabled By SecurityScorecard Ratings and Atlas

MAY 2021

Table Of Contents

Consulting Team: Reggie Lau
Director



Executive Summary

In 2020, a range of public and private organizations across all sectors experienced major data breaches.[1] The cost of data breaches is well documented and, for most industries, the average is more than $3 million per incident.[2] These costs can increase when third parties are the source or involved in other ways. As organizations continue to embrace digital transformation and engage with more technology partners, it is vital to have solutions to rate and monitor third-party risk.

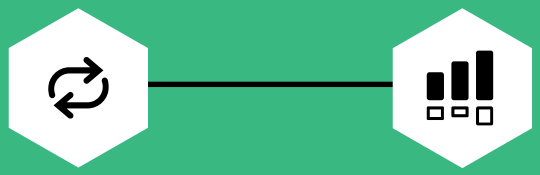
SecurityScorecard Ratings allows organizations to continuously monitor their own cybersecurity health and that of third parties in their ecosystem and supply chain. SecurityScorecard Atlas is an automated questionnaire solution that enables chief information security officer (CISO) teams to gain internal views on security profiles and risks from third parties.

SecurityScorecard commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Ratings and Atlas.[3] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of these SecurityScorecard solutions on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four customers with experience using SecurityScorecard Ratings and Atlas. For the purposes of this study, Forrester aggregated the experiences of the interviewed customers and combined the results into a composite organization. The composite organization will be referred to as Laud National Bank. Use cases and financial modeling in this study are primarily based on tracking cybersecurity risk from third-party relationships.

Prior to using SecurityScorecard, Laud National Bank did not have an automated cybersecurity ratings solution for third-party risk management (TPRM) and leveraged a service provider to manually build vendor profiles. Any processes that existed were informal and ad hoc at best, and questionnaires relied on large spreadsheets that were difficult for vendors to navigate — and even more difficult for the security and risk teams to manage. Without an automated solution to measure third-party ecosystem risk, the company worried about its security posture and regulatory reporting requirements.

KEY STATISTICS



Return on investment (ROI)
198%

Net present value (NPV)
$625K

After the investment in SecurityScorecard, Laud National Bank deploys a formal process and technology that provides consistent and efficient visibility into ecosystem risk and a vehicle to investigate and discuss with vendors. This strengthened the bank's overall security apparatus and posture.

Reduction in vendor questionnaire preparation time and effort
83%

KEY FINDINGS

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

- **Increased efficiency in risk management with savings of $822,791.** TPRM is not an easy task without formal process and an automated platform to support security and risk professionals. SecurityScorecard helps with assessing the cybersecurity aspect of TPRM. Laud National Bank the population of critical vendors to monitor grew twofold over a three-year period. At the same time, the portion of the security and risk team with a TPRM remit remained at five FTEs throughout the three-year period, allowing the composite to scale workload without proportionately scaling hiring costs. The vendor survey questionnaire process became formalized and automated, and surveys no longer lived in large, convoluted spreadsheets, which made assessments easier for vendors to complete and reduced staff time required for follow-ups. This reduced preparation time needed per assessment by 83%. The time and effort related to manual discovery of impacted vendors after major security events in the market also decreased from three FTEs for one week to two hours for coordination.
- **Technology efficiencies and consolidation that led to $118,125 in savings.** With technology investments, organizations can decommission, discontinue, or consolidate certain platforms or services. In the case of the composite, SecurityScorecard fully replaced a legacy manual ratings service provider.

> **Over the past three years, our IT services have tripled, and technology vendor contracts increased by 35% last year. At the same time, we haven't hired anyone new in the past three years to support TPRM.**
>
> — Information security advisor, global energy company

> **We had 10 to 15 vendors related to a major industry breach last year. SecurityScorecard helped us save a week in discovery time and shortened the cycle to survey and follow up with vendors.**
>
> — Deputy CISO, regional financial services provider

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

- **Improved security posture.** Organizations should consider improved security posture as a foundation when building business cases related to security and risk investments. If an organization has not experienced a breach or have historically referenceable costs for a breach for modeling, then average industry figures should be leveraged. Cost of a data breach of over $3 million per incident is a widely circulated reference point.[4] The foundation of a security investment should be firmly planted in the need to improve security posture, which can be generally modeled based on cost components (e.g., revenue impact, reputation impact, professional services and audit fees, fines and penalties, lawsuits) multiplied by breach probability and a prevention attribution ratio.

Costs. Risk-adjusted PV costs include:

- **SecurityScorecard solution cost of $315,379.** As interviewed customers noted that learning to use the platform was intuitive and required immaterial training time, the majority of modeled costs are related to SecurityScorecard's solution cost. This includes three components: Ratings slots, Atlas credits, and customer success.

The customer interviews and financial analysis found that the composite organization experiences benefits of $940,916 over three years versus costs of $315K, adding up to a net present value (NPV) of $625,537 and an ROI of 198%.

ROI
198%

BENEFITS PV
$941K

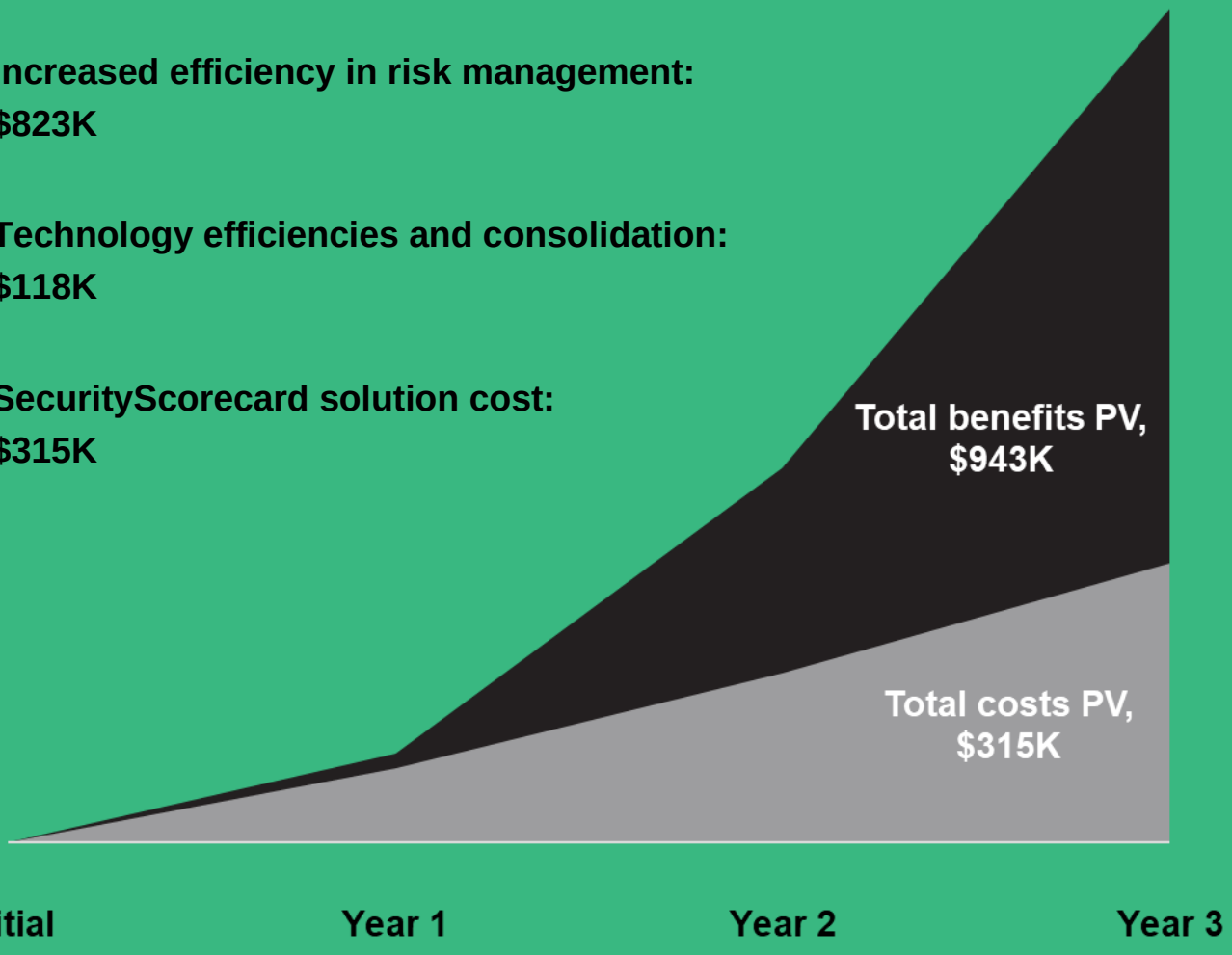
NPV
$626K

PAYBACK
< 3 months

Increased efficiency in risk management:
$823K

Technology efficiencies and consolidation:
$118K

SecurityScorecard solution cost:
$315K



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 SecurityScorecard.

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 SecurityScorecard can have on an organization.

DUE DILIGENCE

Interviewed SecurityScorecard stakeholders and Forrester analysts to gather data relative to SecurityScorecard Ratings and Atlas.

CUSTOMER INTERVIEWS

Interviewed four decision-makers at organizations using SecurityScorecard 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 the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The SecurityScorecard Customer Journey

Drivers leading to the SecurityScorecard Ratings and Atlas investment

Interviewed Organizations

Industry	Region	Critical Vendors	Interviewee
Financial services	US	80	Deputy CISO
Energy	Global	380	Information security advisor
Healthcare	US	10	Senior information security analyst
Financial services	Global	80	Vendor risk manager

KEY CHALLENGES

Prior to deploying SecurityScorecard, most interviewees' organizations had a combination of informal, manual processes and nonexistent or inefficient tools. Some customers used vendor management or governance, risk, and compliance (GRC) software to monitor vendors, but lacked a thorough system to evaluate the cybersecurity risk of third parties. Others leveraged service providers that manually built profiles. Across all interviewees, surveys were mostly executed with email and spreadsheets without any automation.

The interviewees' organizations struggled with common challenges, including:

- **Growing volume of third-party relationships and no way of consistently and efficiently rating third-party cybersecurity postures.** Interviewees' organizations increased their vendor ecosystem as more viable options became readily available to support various digital transformation initiatives. Security and risk naturally became a priority on digital transformation roadmaps — not only to secure each company's properties, but also to provide visibility into the broader ecosystem's posture and meet regulatory and compliance demands. It became no longer pragmatic to manage hundreds or thousands of critical vendors without a scalable cybersecurity risk rating solution. While service providers manually developing vendor profiles by request was a legacy option, it was not scalable based on cost or timeliness.
- **Survey questionnaires and processes were manual, labor intensive, confusing for vendors, and ad hoc.** Relying on large spreadsheets confused some survey respondents, leading to them abandoning their response. This would delay the process and require the interviewees to spend more time and effort to follow up and provide clarification. Once answers came back, managing multiple large spreadsheets was also cumbersome and

> **"Before SecurityScorecard, we had a third-party service provider to manually assess vendors. If we brought it in-house, we would need a lot of people to replicate the capability — and that's just to gather data in public domain for 80 vendors. It doesn't include building out intuitive visualizations or continuous updates."**
>
> *Vendor risk manager, global financial services provider*

interviewees rarely had an efficient and accurate way to validate answers. Aside from the tool, processes dictating workflow, thresholds, and frequency of surveying ranged from ad hoc to informal at best.

SOLUTION REQUIREMENTS/INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that could:

- Monitor critical vendors at scale.
- Provide an easy-to-understand visualization, dashboard, or rating rubric.
- Survey vendors consistently and efficiently in a consolidated, linked, and integrated way.
- Justify decommissioning of less efficient existing solutions.
- Potentially feed into threat intelligence and enterprise risk management.

After evaluating multiple vendors, interviewees' organizations chose SecurityScorecard because of:

- Its efficient, scalable, and packaged solution in Ratings and Atlas that serves multiple purposes.
- Its relatively transparent and simplified pricing.

Its ease of deployment and availability of support.

COMPOSITE ORGANIZATION — LAUD NATIONAL BANK

Based on the interviews, Forrester constructed a TEI framework, a composite company, and a ROI analysis that illustrates the areas financially affected. The composite organization, Laud National Bank, 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 has the following characteristics:

Description of composite. Laud National Bank is a regional bank with $15 billion in assets under management (AUM) and has operations in over 25 US states. The organization provides a range of financial services to both businesses and consumers, including standard checking, savings, loans, and longer-term financial planning and investments.

Prior state and deployment characteristics. Laud National Bank realized that it was signing on more vendors as it embraced the range of digital options and partners as part of its digital transformation roadmap. While security and risk were certainly a part of the roadmap, the company did not anticipate the larger risk exposure that comes with adopting new technologies and onboarding new digital partners. The CIO and CISO elects a lead from the existing information security team to spearhead a new third-party vendor risk management program. Among other duties, this team of five documents existing processes and tools, designs a future vision, evaluates partners who could support the vision, and then selects SecurityScorecard as the platform to realize the future vision. The team forecast accelerates company growth and starts its relationship with SecurityScorecard with 50 continuously monitored critical vendors. The number of critical vendors doubles to 100 Ratings slots in Year 3. This is a similar story with vendor surveys as the company doubles its Atlas credits from 100 to 200 by Year 3.

Key assumptions

- **$15 billion AUM**
- **Operations in over 25 US states**
- **More than100 critical vendors**
- **Five team members with TPRM responsibilities**

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	Improved security posture	-	-	-	-	-
Btr	Increased efficiency in risk management	$63,188	$343,580	$640,739	$1,047,507	$822,791
Ctr	Technology efficiencies and consolidation	$47,500	$47,500	$47,500	$142,500	$118,125
	Total benefits (risk-adjusted)	$110,688	$391,080	$688,239	$1,190,007	$940,916

IMPROVED SECURITY POSTURE

Recommended approach. Forrester's approach in building market-facing TEI models is to ensure actual experiences are quantified and articulated. Since the interviewed customers did not experience breaches due to a third-party vulnerability, this study presents the benefit category of "Improved security posture" as a recommended approach rather than offering general figures and assumptions.

Nevertheless, even if unquantified, an improvement to security posture should be the foundation of a business case for a security-related investment. This is the first area that users should consider when building a business case for SecurityScorecard.

Modeling and assumptions. When building a model for the value of improved security posture, organizations can take advantage of industry reports with data from the past several years. However, using average or consolidated figures that consider all types of breaches and use cases may overstate or understate the value depending on your company's use case and current state. Instead, breakdown the cost of a breach and fill in the estimate and assumptions based on your internal stakeholders' and finance's feedback. These components can be summarized as:

- Revenue impact, typically due to downtime.
- Reputation and brand value impact, typically leading to longer term customer retention or contract renewal revenue impact.
- Increased professional services and audit fees.
- Fines and penalties from regulatory bodies.
- Lawsuits from civil charges.

Consider the values of each with the probability of a breach and the attributed value given to the technology solution for preventing that breach relative to all other components the company has in place to prevent a breach.

> **"A breach isn't just about downtime and customer data — it's innovation, intellectual property, and business secrets. If confidential information about a M&A deal leaked out, that could be worth millions or billions."**
>
> *Information security advisor, global energy company*

Risks. Consider the risks that can reduce the value of the benefit.

- Breach impact, probability, or frequency is less than estimated.
- Greater prevention attribution credited to other components of the security apparatus.

To account for these risks, Forrester suggests using risk ranges or a triangulation method. Please see Appendix A for more details.

Improved Security Posture

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
A1	Revenue impact (short-term)	Based on company estimates	-	-	-
A2	Reputation, brand, and retention impact (long-term)	Based on company estimates	-	-	-
A3	Increased professional services and audit fees	Based on company estimates	-	-	-
A4	Fines and penalties (regulatory)	Based on company estimates	-	-	-
A5	Lawsuits (civil)	Based on company estimates	-	-	-
A6	Breach probability or frequency	Leverage third-party reference	-	-	-
A7	Prevention attribution ratio	Estimated assumption	-	-	-
At	Improved security posture	(A1+A2+A3+A4+A5)*A6*A7	-	-	-
	Risk adjustment	↓10%			
Atr	Improved security posture (risk-adjusted)		-	-	-
	Three-year total: -		**Three-year present value: -**		

INCREASED EFFICIENCY IN RISK MANAGEMENT

Evidence and data. Interviewees' organizations needed a repeatable and scalable way to manage third-party risk. SecurityScorecard provides a rating system and a dashboard that interviewees mentioned were intuitively made for executive consumption. The platform transformed the manual or ad hoc ways that organizations monitored and surveyed vendors.

Modeling and assumptions. Laud National Bank broke down its risk management efficiency into three parts:

- The first part is related to an accelerated growth in vendor relationships and critical vendors that need monitoring. The critical vendor volume increases from 50 to 100 in a three-year period, but the size of the team remains the same throughout that period. This allows Laud National Bank to avoid hiring 2.5 to 5 FTEs during that period.
- The second component is related to the formalization and efficiency in administering vendor survey questionnaires. SecurityScorecard

Atlas replaces large offline spreadsheets and makes the user experience more friendly and intuitive for vendors. This results in shorter cycle times and fewer follow-ups. The composite estimates an 83% reduction in time needed, reducing 60 minutes of material work to 10 minutes.

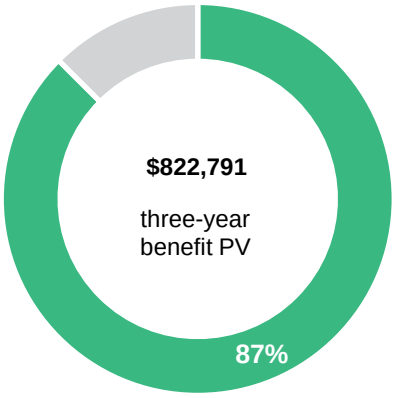
- Finally, SecurityScorecard informs Laud National Bank about vendors potentially related to major breach events during the year. In the past, the composite would either perform a cursory job of checking links between its ecosystem and the breach or it would take 3 FTEs one week to perform a proper discovery. Since SecurityScorecard provides this information, the team no longer has to manually conduct discovery and really just needs a two-hour coordination call to plan for vendor outreach.

Risks. Consider the risks that can reduce the value of the benefit.

- Further increments of critical vendors in future years may necessitate incremental hires, even if hiring costs are disproportionately favorable and less than vendors onboarded.
- Speed and frequency of SecurityScorecard updates could affect the speed in which the composite conducts its discovery after a major breach event in the industry. If the speed is slower than needed, the composite could ultimately revert back to the manual discovery process.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $822,791.

Increased Efficiency In Risk Management



"Sometimes, you just don't know what you don't know. But with SecurityScorecard, now we know — so we have something to discuss and talk about with vendors. Sometimes, they don't even know about their own vulnerabilities or encryptions that haven't been updated."

Senior information security analyst, regional healthcare company

Increased Efficiency In Risk Management					
Ref.	**Metric**	**Calculation**	**Year 1**	**Year 2**	**Year 3**
B1	Critical vendors monitored	Composite	50	75	100
B2	FTEs needed without SecurityScorecard	Composite	5.0	7.5	10.0
B3	FTEs avoided with SecurityScorecard	$B2_{cy}$-$B2_{year\ 1}$	0.0	2.5	5.0
B4	Annual salary	Year 1: Assumption Year 2 and 3: $B4_{py}$*103%	$108,000	$111,240	$114,577
B5	Cost avoidance while scaling TPRM program	B4*B3	$0	$278,100	$572,885
B6	Assessments per year	Composite	100	150	200
B7	Prior preparation time per assessment (minutes)	Composite	60	60	60
B8	Preparation time saved per assessment	Composite	83%	83%	83%
B9	Preparation time per assessment (minutes)	B7*(1-B8)	10.2	10.2	10.2
B10	Assessment cost saving	(((B7-B9)*B6)/60)*(B4/2,080)	$4,310	$6,658	$9,144
B11	Critical events per year	Year 1: Assumption Year 2 and 3: $B11_{py}$*120%	10	12	14
B12	FTE coverage	Composite	3	3	3
B13	Discovery hours	Composite	40	40	40
B14	Total discovery hours without SecurityScorecard	B11*B12*B13	1,200	1,440	1,680
B15	Coordination hours with SecurityScorecard	Composite	2	2	2
B16	Discovery cost avoidance	(B14-B15)*(B4/2,080)	$62,204	$76,905	$92,433
Bt	Increased efficiency in risk management	B5+B10+B16	$66,514	$361,663	$674,462
	Risk adjustment	↓5%			
Btr	Increased efficiency in risk management (risk-adjusted)		$63,188	$343,580	$640,739
Three-year total: $1,047,507		**Three-year present value: $822,791**			

TECHNOLOGY EFFICIENCIES AND CONSOLIDATION

Evidence and data. When building business cases, many users often forget to include the costs that they no longer need to pa such as a refresh cost, recurring subscription, or maintenance fee. In this case, Laud National Bank wants to consolidate some disparate pieces of software that had similar functionality and discontinue engagement with a service provider that manually built vendor profiles by request.

As the information security team investigates the applications for consolidation, the team realizes that each piece still has some unique function and the product owners are not readily willing to give up

control or to decommission their usage. The team scraps its plans for consolidation and proceeds with only the discontinuing of its service provider for vendor profiles.

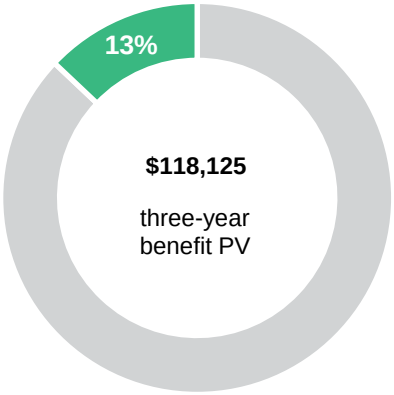
Modeling and assumptions. All software, hardware, and services or combination of these components that can be consolidated, discontinued, or decommissioned should be included in this portion of the model. Items with recurring fees, recurring maintenance labor, or upcoming refresh or one-time costs that are reasonable to include in a three-year model should be accounted for. If decommissioning a component does not materially affect costs or labor, then it can potentially be excluded.

Risks. Consider the risks that can reduce the value of the benefit.

- Challenges in consolidation efforts due to resistance to change.
- Components to be decommissioned do not carry any recurring cost or labor implication.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $118,125.

Technology Efficiencies And Consolidation



Technology Efficiencies And Consolidation

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
C1	Legacy manual ratings volume	Composite	25	25	25
C2	Cost per manual rating	Composite	$2,000	$2,000	$2,000
C3	Third-party manual risk rater cost avoidance	C1*C2	$50,000	$50,000	$50,000
Ct	Technology efficiencies and consolidation	C3	$50,000	$50,000	$50,000
	Risk adjustment	↓5%			
Ctr	Technology efficiencies and consolidation (risk-adjusted)		$47,500	$47,500	$47,500
	Three-year total: $142,500		**Three-year present value: $118,125**		

FLEXIBILITY

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

- **Enterprise risk management**. For at least one of the interviewees, SecurityScorecard was deployed first as an enterprise risk management tool to track any public vulnerabilities of the company. Two of the interviewees mentioned that this would be a use case they would consider going forward.
- **Threat intelligence**. One of the interviewees found early success in combining SecurityScorecard data with other sources of threat intelligence for a more comprehensive and holistic view. Going forward, the customer plans to formally use SecurityScorecard for this purpose.
- **Tighter usage of Ratings and Atlas together**. All four interviewees used both Ratings and Atlas. One interviewee still flipped back and forth between Atlas and an existing survey tool built into another application. With tighter integration of Ratings and Atlas, this interviewee plans to test more consistent use of Atlas.
- **Cyber insurance premiums.** Many cyber insurance vendors now use ratings scores to set premiums. Organizations that proactively manage enterprise and critical third-party vendor scores are likely to see lower premiums.

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

“The dashboard and reporting are easy enough for executives to understand. Our CISO looks at it whenever he wants and then brings the scores up to show the CEO. It’s pretty much self service.”

— Vendor risk manager, global financial services provider

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**
Dtr	SecurityScorecard solution cost	$0	$92,400	$129,150	$165,900	$387,450	$315,379
	Total costs (risk-adjusted)	$0	$92,400	$129,150	$165,900	$387,450	$315,379

SECURITYSCORECARD SOLUTION COST

Evidence and data. The primary cost for SecurityScorecard is SecurityScorecard itself. The deployment, training, and any other costs or time and labor considerations were immaterial in each of the interviewees' cases.

Modeling and assumptions. Laud National Bank considers three components in its SecurityScorecard solution cost.

- The first is the cost per Ratings "slot" or a total cost based on quotation from SecurityScorecard.
- The second is the cost per Atlas credit or a total cost based on quotation from SecurityScorecard.
- Lastly, though there was no additional cost in this case, users should verify if there might be a cost for a customer success manager or any type of "premium" service.

Readers should contact SecurityScorecard for the most updated and tailored solution cost.

Risks. As the cost for this solution is quite straightforward, the largest risk consideration users should build into this model is whether the organization may need more Ratings slots and Atlas credits than planned. This risk should be proportional to the probability that growth in the company's vendor relationships will outpace its plan.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $387,450.

SecurityScorecard Solution Cost						
Ref.	**Metric**	**Calculation**	**Initial**	**Year 1**	**Year 2**	**Year 3**
D1	Ratings slots	B1		50	75	100
D2	Ratings cost	SecurityScorecard provided		$63,000	$85,500	$108,000
D3	Atlas credits	B6		100	150	200
D4	Atlas cost	SecurityScorecard provided		$25,000	$37,500	$50,000
D5	Customer success manager fee	SecurityScorecard provided		$0	$0	$0
Dt	SecurityScorecard solution cost	D2+D4+D5	$0	$88,000	$123,000	$158,000
	Risk adjustment	↑5%				
Dtr	SecurityScorecard solution cost (risk-adjusted)		$0	$92,400	$129,150	$165,900
	Three-year total: $387,450			**Three-year present value: $315,379**		

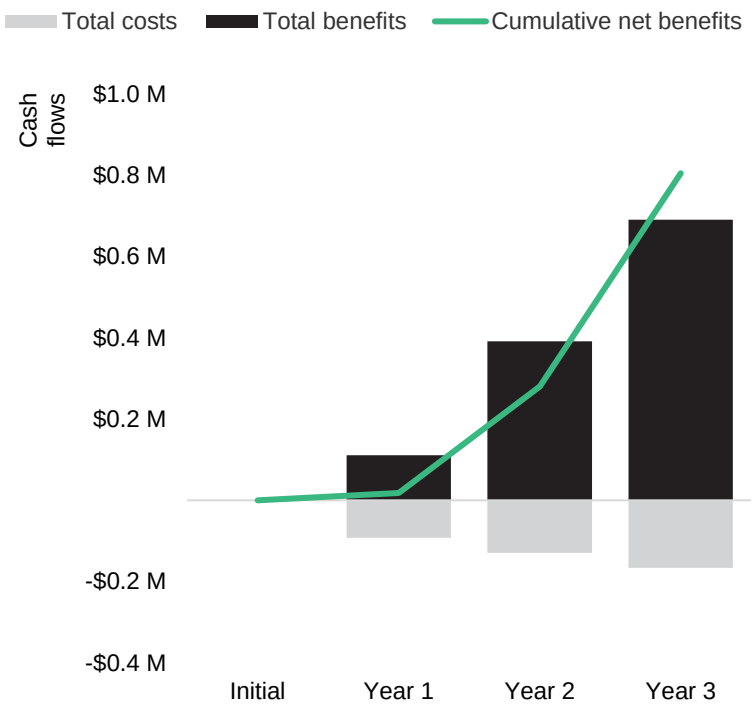
“Buy for scale and budget for what you might need three to five years from now to account for digital acceleration.”

— Information security advisor, global energy company

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	$0	($92,400)	($129,150)	($165,900)	($387,450)	($315,379)
Total benefits	$0	$110,688	$391,080	$688,239	$1,190,007	$940,916
Net benefits	$0	$18,288	$261,930	$522,339	$802,557	$625,537
ROI						198%
Payback period (months)						< 3

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: Supplemental Material

Related Forrester Research

“The Forrester New Wave™: Cybersecurity Risk Ratings Platforms, Q1 2021,” Forrester Research, Inc., February 25, 2021.

“The Forrester Wave™: Third-Party Risk Management Platforms, Q4 2020,” Forrester Research, Inc., October 6, 2020.

“Planning For Failure: How To Survive A Breach,” Forrester Research, Inc., August 19, 2020.

“Now Tech: Third-Party Risk Management Technology, Q3 2020,” Forrester Research, Inc., August 5, 2020.

“The Forrester Wave™: Supplier Risk And Performance Management Platforms, Q3 2020,” Forrester Research, Inc., July 28, 2020.

“Now Tech: Supplier Risk And Performance Management (SRPM), Q2 2020,” Forrester Research, Inc., June 29, 2020.

“The Forrester New Wave™: Cybersecurity Risk Rating Solutions, Q4 2018,” Forrester Research, Inc., November 13, 2018.

Appendix C: Endnotes

[1] Maria Henriquez, “The top 10 data breaches of 2020,” Security Magazine, December 3, 2020 (https://www.securitymagazine.com/articles/94076-the-top-10-data-breaches-of-2020).

[2] “Cost of a Data Breach Report 2020,” Ponemon Institute, July 2020.

[3] 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

[4] “Cost of a Data Breach Report 2020,” Ponemon Institute, July 2020.


FORRESTER®