A Forrester Total Economic Impact™
Study Commissioned By Acronis
August 2019

The Total Economic Impact™ Of Acronis Cyber Protection

Cost Savings And Business Benefits Enabled By Acronis Cyber Protection

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®

Benefits Highlights

Based on interviews with the chief information officer for a high-performance manufacturing firm

Annual time savings for IT operations staff in backup and recovery workflows:

1,200 hours

Annual cost savings over alternative solutions for 4.5 million GBs of cloud storage capacity and data protection:

$1 million

Executive Summary

As competition to win, serve, and retain customers continues to intensify, it will become increasingly important to ensure the uptime and availability of business-critical systems and infrastructure. While most companies have firm plans in place to deal with business disruption caused by earthquakes, floods, and other catastrophic events, many remain vulnerable to business disruption perpetuated by malicious actors and agents.[1]

According to recent reports from global brands, costs associated with a ransomware attack can climb to tens or hundreds of millions of dollars, once businesses account for the full scope of damages.[2] Despite these high costs, only 63% of information professionals surveyed in Forrester's Q3 2017 Global IT Business Continuity And Disaster Recovery Preparedness Online Survey said that their organizations' business continuity plans included contingencies for recovering from a ransomware attack.[3] What's more, only 36% said that they were very confident in their organizations' ability to recover from a ransomware attack.

Acronis Cyber Protection solutions enable customers to protect mission-critical data from cyberthreats and malicious agents, while ensuring that data is readily accessible to support the business. Acronis commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment enterprises may realize by deploying an Acronis Cyber Protection solution. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Acronis Cyber Protection solutions on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed the chief information officer for a manufacturer of high-performance equipment, which has been using Acronis' Cyber Protection solutions for approximately two years to store and protect the significant volumes of data generated by the design, testing, and deployment of its products.

Prior to implementing the Acronis Cyber Protection solution, the interviewed organization leveraged a combination of magnetic tape and hybrid cloud solutions to back up some business-critical data. The former was time-consuming and inefficient to operate, and the latter was costly to scale, since not all of the organization's data was fit for archive-tier storage. More importantly, however, the organization's preexisting approach to data storage left backups vulnerable to ransomware attacks, which had infected user machines on two occasions in the past.

For this organization, the Acronis Cyber Protection solution was a critical component in a layered approach to protecting intellectual property from malicious actors. (At the same time the organization invested in Acronis, it also invested in network security and threat detection solutions.) The chief information officer told Forrester, "Whereas two years ago, I reported to the board that I couldn't guarantee that our data and infrastructure was protected from an attack, I now feel confident in saying that we have built several layers of security protection and done as much as we possibly can to protect the business." While being able to store backup data securely was a primary requirement, the organization was also able to procure enough capacity to ensure that it could back up the vast amounts of data being generated by the business, without incurring additional costs if it needed to access that data.

ROI
47%

Benefits PV
$8.0M

NPV
$2.5M

Payback
< 6 months

Key Findings

Quantified benefits. The interviewed organization experienced the following risk-adjusted present value (PV) quantified benefits:

- **Backup and recovery workflow time savings totaling $109,329.** The Acronis Cyber Protection solution reduced the amount of time IT operations staff spent on routine backup and recovery tasks, freeing up time for other value-added activities.
- **Estimated avoided costs of ransomware attacks totaling $321,524.** According to the chief information officer for the interviewed organization, the Acronis Cyber Protection solution reduced the likelihood of business disruption associated with ransomware attacks by 1) ensuring the integrity of backup data and 2) ensuring that any data created by the organization could be quickly restored to keep the business running.
- **Estimated avoided costs for cloud storage capacity totaling $7,570,137.** The Acronis Cyber Protection solution enabled the interviewed organization to back up and secure its data at a substantially lower cost than scaling up its use of a preexisting cloud storage solution. On an annual basis, the organization pays $1 million less for the Acronis Cyber Protection solutions than it would have paid for the same 4.5 million GBs of capacity from its preexisting cloud storage provider. (Costs to procure storage capacity from Acronis are shown in the cost section of this analysis.)

Unquantified benefits. The interviewed organization experienced the following benefits, which were not quantified for this study:

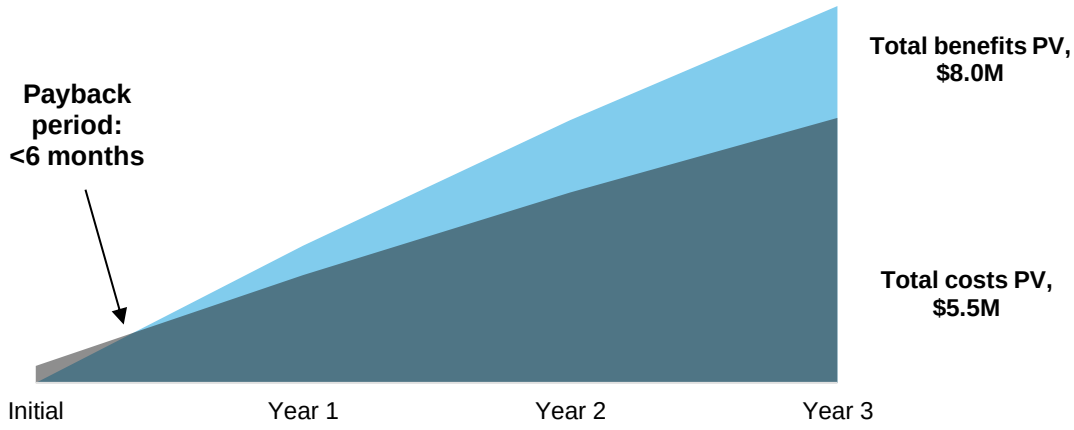
- **Avoidance of extreme business disruption and reputational damage.** In the financial benefits section of this case study, Forrester quantifies the avoided cost of small-scale business disruption associated with a ransomware attack and the temporary interruption in access to data that supports revenue-generating projects. However, we do not attempt to quantify the avoided cost of a significant disruption to business activities (e.g., the inability to deliver a product on schedule) or the loss of key customer accounts due to a loss in trust.
- **More comprehensive data backups, which provide employees with access to data they need to do their jobs.** Prior to adopting the Acronis Cyber Protection solution, it could take IT operations staff days to fulfill a data recovery request, leaving employees without data essential to move projects forward. In some cases, data couldn't be recovered at all because either 1) the data wasn't backed up in the first place or 2) the data was routinely discarded after a set period of time due to storage limits. The Acronis Cyber Protection solution enables the organization to more thoroughly back up its data and restore files promptly upon request. However, the impact on productivity of having access to complete file histories is difficult to quantify and is not represented in the financial benefits section of this analysis.
- **Better organizational resilience.** In the event that one of the organization's data centers goes offline, Acronis enables IT staff to replicate it in a matter of hours. The interviewed organization has two onsite data centers. In the event that one goes down, it can restore everything stored in the failed environment to the one that's fully functioning, ensuring that critical systems are available to the business. According to the chief information officer, the organization lacked these capabilities in the past, and it was vulnerable to disruption in operations.

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

- **Fees paid to Acronis over three years totaling $5,448,047.** The interviewed organization paid one-time fees to Acronis for professional services and implementation support. It also pays ongoing fees for cloud storage capacity and access to Acronis software solutions.
- **Additional implementation costs totaling $5,077.** To a large extent, Acronis' professional services team oversaw the setup and implementation process, and these costs are reflected in the section titled Fees Paid To Acronis. However, the interviewed organization did incur nominal costs for time spent on planning, implementation, and training activities over the course of 12 weeks.

Forrester's interviews with this customer and subsequent financial analysis found that the interviewed organization experienced benefits of $8.0 million over three years versus costs of $5.5 million, adding up to a net present value (NPV) of $2.5 million and an ROI of 47%.

Financial Summary



FORRESTER®

TEI Framework And Methodology

From the information provided in the interviews, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing an Acronis Cyber Protection solution.

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 Acronis Cyber Protection 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 Acronis stakeholders and Forrester analysts to gather data relative to Acronis Cyber Protection solutions.

CUSTOMER INTERVIEW
Interviewed one organization using Acronis Cyber Protection solutions to obtain data with respect to costs, benefits, and risks.

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

CASE STUDY
Employed four fundamental elements of TEI in modeling the impact of Acronis Cyber Protection solutions: 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.

The Acronis Cyber Protection Customer Journey

BEFORE AND AFTER THE INVESTMENT IN AN ACRONIS CYBER PROTECTION SOLUTION

Interviewed Organization

For this study, Forrester conducted multiple interviews with the chief information officer for a high-performance manufacturing business. The business, which earns approximately $230 million in annual revenues, is a data-intensive one. At every stage of the production process, from design to testing to deployment, the business generates high volumes of data. It leverages this data for the continuous improvement of its products.

The following high-level metrics describe the organization from a people and technology perspective:

- 1,000 employees, 60% of whom work remotely.
- 25 IT employees, with a total of five IT employees dedicated to IT operations.
- 2,000 endpoint devices, including end user laptops as well as laptops embedded in manufacturing workstations.
- 25 Nutanix appliances.
- 720 virtual machines (VMs): 600 VMs that power critical infrastructure and 120 VMs that support the virtual desktop environment, including computer-aided design (CAD) software.

> "Before this upgrade, I couldn't stand before the board of the company and say that we would be able to recover any piece of data. Now I can say that."
>
> *Chief information officer, high-performance manufacturing company*

How The Organization Is Leveraging Acronis

For the interviewed organization, the Acronis investment was part of a comprehensive overhaul to how the company protects proprietary data. To improve frontline protection against malicious agents, the organization invested in an advanced threat-detection solution as well as an improved network security solution. The Acronis Cyber Protection solution, which the organization purchased to ensure the integrity and security of its backup data, was the third pillar of this strategy.

The interviewed organization uses the Acronis Cyber Protection solution to back up and secure data from the following sources:

- **Endpoint devices.** Ensuring that a backup exists for all desktop files, including all large CAD files.
- **Email and file systems.** Ensuring that all mailboxes, spreadsheets, and other files stored in the company's corporate directory can be quickly restored from backup.
- **Physical and virtual servers.** Ensuring that a backup exists for all data stored in the company's two onsite data centers and that data can be quickly mirrored to one of the data centers should the other go down temporarily.

> "We've literally gone from a situation where it might take us days to recover data, to one where it takes just minutes. We're able to restore data with a lot of precision, right down to a single file or a single email."
>
> *Chief information officer, high-performance manufacturing company*

FORRESTER®

Key Challenges

The interviews revealed the following key drivers for the investment in an Acronis Cyber Protection solution:

- **Executing backup routines was time-consuming, and there was always a backlog of data slated for backup.** Prior to implementing the Acronis Cyber Protection solution, the interviewed organization leveraged a magnetic tape storage solution to back up the volumes of data generated by its high-performance manufacturing business. While cost-effective, the magnetic tape solution required the attention of two members of the IT operations staff, who together spent roughly 20 hours per week on administrative tasks (e.g., starting and stopping backups, migrating tapes to safe storage). Since the read/write speeds on the magnetic tape storage solution were so slow, and one backup routine was often incomplete when the next was scheduled to start, there was always a backlog of data that needed to be backed up.
- **Data recovery requests could take days to fulfill.** Prior to the Acronis implementation, employee requests for data recovery and restoration could take days to fulfill. To meet a request, IT operations staff had to locate data in its tape storage archive, and this was a tedious process. In the meantime, users went without files they needed to move projects forward.
- **Scaling the organization's use of its preexisting cloud storage solution would be costly.** Prior to the Acronis implementation, the interviewed organization procured 1PB of storage capacity from a public cloud vendor. While this solution was reasonably cost-effective for archive-tier data, costs were higher for files and data that the organization needed to access more frequently. To scale up this model and procure enough capacity for all of the organization's data would have been expensive.
- **Vulnerability to ransomware attacks was an ongoing concern.** In the two years prior to the Acronis implementation, the interviewed organization was the victim of ransomware attacks on two separate occasions. In both instances, the attacks were relatively isolated, and backups were available for all of the files encrypted by the malware. However, the attacks created concerns at the executive and board levels that future attacks could have a significant and negative impact on the business. These concerns were well-founded: Over the last several years, global brands have reported costs associated with ransomware attacks in the tens or hundreds of millions of dollars.[4]
- **Employees' data was vulnerable to loss.** Prior to implementing the Acronis Cyber Protection solution, files and data generated by remote workers weren't always backed up, owing to the inadequacy of the organization's preexisting endpoint backup solution. Even though 60% of the workforce (including CAD designers) regularly works away from the primary site, data was only backed up completely when employees were onsite. When employees were offsite, per-user storage limits went into effect to ensure that performance of users' machines didn't suffer. In addition, some file types (e.g., file types that tended to be very large) were excluded from backup routines, since they tended to cause machines to lag. As a result, data generated by employees when they were offsite was vulnerable to loss.

> "If the ransomware had gotten further along before we detected it, and it had started to encrypt files that we couldn't recover, the result could have been very damaging to the business. We got lucky that the person whose machine was compromised had access to less data than many others."
>
> *Chief information officer, high-performance manufacturing company*

> "[Before the Acronis implementation], there was a huge risk that a piece of malware could take down the company. Now, 18 months after the Acronis implementation, I can go back to the board and say that we've done everything possible to protect our data from an attack."
>
> *Chief information officer, high-performance manufacturing company*

Solution Requirements

Prior to implementing the Acronis Cyber Protection solution, the interviewed organization sought a solution that would allow it to do the following:

- Back up on a continuous basis all of the organization's data, including data stored 1) in the organization's two onsite data centers, 2) in emails and the corporate directory, and 3) on users' laptops.
- Provide an added layer of protection against ransomware and other malicious agents.
- Reduce the amount of time IT operations staff spent on data backup and recovery-related tasks.

Key Results

The chief information officer for the interviewed organization described the following key results from the investment in an Acronis Cyber Protection solution:

- **Automated backup routines.** According to the chief information officer, data backup routines are now largely automated. IT operations staff spend only about 90 minutes each week monitoring log files for exceptions.
- **The ability to quickly restore data.** In most cases, end users can retrieve files from backup themselves. When they need a file that's been archived, they'll still need to work with the IT operations staff. However, for IT staff, the process of retrieving a file from backup now involves only a few clicks, as opposed to a search through the organization's magnetic tape storage archive. The chief information officer told Forrester, "We're now able to complete requests for data recovery — down to a single email or a single file from storage — in minutes rather the days it was taking us before the Acronis upgrade."
- **Systems simplification.** Whereas before the interviewed organization used three separate systems for backup and recovery across the data centers, cloud, and user endpoints, it now relies on Acronis for all of these capabilities. For IT staff, this translates to less administrative overhead and ongoing training costs.
- **Cost-effective data storage and protection.** With Acronis, the interviewed organization was able to procure enough capacity to back up and secure all of the data generated by its high-performance manufacturing business at a cost that was significantly less than scaling up usage of its preexisting cloud storage solution. To procure the same 4.5 million GBs of capacity from the prior cloud storage vendor, the interviewed organization would have paid $1.05 million more on annual basis.

Analysis Of Benefits

QUANTIFIED BENEFIT DATA

Total Benefits

REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Backup and recovery workflow time savings	$42,750	$44,033	$45,353	$132,136	$109,329
Btr	Avoided cost of ransomware attacks	$124,460	$129,535	$134,864	$388,859	$321,524
Ctr	Avoided costs for alternative solution	$3,074,200	$3,026,700	$3,026,700	$9,127,600	$7,570,137
	Total benefits (risk-adjusted)	$3,241,410	$3,200,268	$3,206,918	$9,648,595	$8,000,990

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 interviewed organization expects risk-adjusted total benefits to be a PV of approximately $8.0 million.

With Acronis, backup routines are largely automated. Similarly, data recovery tasks are largely self-service, and end users can retrieve data without assistance from IT operations staff.

Backup And Recovery Workflow Time Savings

The Acronis Cyber Protection solution reduced the amount of time IT operations staff spent on routine backup and recovery tasks, freeing up time for other value-added activities.

Backup Routines

Prior to implementing the Acronis Cyber Protection solution, IT operations staff at the interviewed organization spent approximately 20 hours each week on backup-related tasks (e.g., administration activities, starting and stopping data transfers, migrating magnetic tapes to safe storage). While the magnetic tape storage solution was cost-effective, it wasn't adequate to serve the evolving needs of the business, owing to the rate at which normal business operations generated data. Oftentimes, backup routines took longer than the scheduled window to complete, creating a lengthy backlog.

With Acronis, backup routines are largely automated. Once a day, the IT operations staff reviews a report, which highlights exceptions and issues. Reviewing reports requires less than an hour each day, according to the chief information officer.

Recovery Workflows

Prior to implementing the Acronis Cyber Protection solution, requests for data recovery came in on a weekly basis, and they consumed at least half a day for IT operations staff. During this time, IT staff had to locate files from tape storage and, when files weren't available in the tape backup, attempt to partially restore them from the most recent incremental backup.

Now, data recovery tasks are largely self-service, and end users can retrieve files without assistance from IT operations staff. In some instances, where users aim to recover a file from archive storage, they may still need to request assistance. However, IT staff can fulfill these data recovery requests in minutes, since doing so "only requires a few clicks."

The following assumptions are represented in the financial model for this benefit category:

- Prior to implementing the Acronis Cyber Protection solution, IT operations staff at the interviewed organization spent approximately 24 hours on routine backup and recovery tasks each week.
- With the Acronis Cyber Protection solution in place, IT operations staff at the interviewed organization complete routine backup and recovery tasks in approximately 1.5 hours.

The following factors may also contribute to variability in the impact of this benefit category:

- An organization's preexisting approach to data backup and recovery and the extent to which that approach enables efficient workflows.
- The extent to which end users are comfortable executing recovery workflows without requesting assistance from IT.

To account for this variability, Forrester applied a risk adjustment of 5%, yielding a three-year, risk-adjusted total PV of $109,329.

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.

Backup And Recovery Workflow Time Savings: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
A1	Weekly hours spent on data backup prior to Acronis implementation	Customer interview	20	20	20
A2	Weekly hours spent on data recovery prior to Acronis implementation	Customer interview	4	4	4
A3	Weekly hours spent on data backup and recovery workflows with Acronis	Customer interview	1.5	1.5	1.5
A4	IT operations analyst hourly rate, fully burdened (rounded)	3% annual increase	$38.46	$39.62	$40.80
At	Backup and recovery workflow time savings	((A1+A2)-A3)*52*A4	$45,000	$46,350	$47,741
	Risk adjustment	↓5%			
Atr	Backup and recovery workflow time savings (risk-adjusted)		$42,750	$44,033	$45,353

Avoided Cost Of Ransomware Attacks

According to the chief information officer, the Acronis Cyber Protection solution reduced the potential for business disruption associated with a ransomware attack.

Prior to implementing the Acronis Cyber Protection solution, as well as several other layers of data security, the interviewed organization experienced ransomware attacks on two separate occasions. In both cases, IT staff isolated the malware attack before it encrypted files that couldn't be recovered. However, the chief information officer acknowledged that this was the result of luck, as the organization didn't have a complete backup of all of its business-critical data.

The potential impact of a ransomware attack that encrypts unduplicated data is difficult to discern. In a best-case scenario, no data would be exposed outside the organization, and access to encrypted files could be restored simply by paying the ransom. Projects would suffer only temporary delays while IT staff, in collaboration with other key stakeholders in the organization, worked to restore file access. In a worst-case scenario, where data is permanently lost or exposed outside the organization, the business could suffer significant project delays, reputational damage, and the loss of customer accounts. Instances of the latter have been widely cited in the news media, with some organizations reporting ransomware-related damages in the tens-of-millions of dollars.[5]

Since Acronis enables the organization to quickly restore files, while also ensuring the integrity of those files, it limits the possibility that the organization will face significant business disruption as a result of a ransomware attack.

The following assumptions are represented in the financial model for this benefit category:

- The potential impact of a ransomware attack is estimated using the organization's daily operating revenue, the number of critical projects potentially impacted by such an attack, and the time-to-resolution for a ransomware attack. (The time-to-resolution is based on the organization's past experience in resolving ransomware attacks.)
- For example, the calculation of the potential business impact of a ransomware attack (B5) in Year 1 assumes 1) a daily revenue rate of $884,615, 2) 260 annual operating days, 3) that 5% of critical projects could be impacted by a ransomware attack, and 4) a five-day timeline to restore access to project-critical files in the wake of a ransomware attack. The potential business impact of a ransomware attack (B5) grows over the three-year period of analysis, owing to the 5% growth in top-line revenues shown in B1.
- By improving data security, the organization also avoids post-attack reviews, which have historically required time from the organization's technical and executive leadership. This model conservatively estimates the cost of a post-attack review at $50,000.

In a worst-case scenario, where data is permanently lost or exposed outside the organization, the business could suffer significant project delays, reputational damage, and the loss of customer accounts.

- To produce a conservative estimate of the potential business impact of a ransomware event, this model assumes that even in the absence of the Acronis Cyber Protection solution, there is not a 100% chance that the organization will face a successful ransomware attack. Further, it assumes that the likelihood of the organization experiencing a successful ransomware attack is equal to the percentage of organizations (51%) that experienced a ransomware attack over the prior 12 months, as cited in the Ponemon Institute's study titled The Rise Of Ransomware (September 2017).[6]

The following factors may also contribute to variability in the impact of this benefit category:

- The frequency with which an organization is the target of ransomware attacks.
- The extent to which threat detection and network security solutions are effective in preventing ransomware attacks.
- The extent to which an organization's employees follow best practices designed to prevent ransomware infections.

To account for this variability, Forrester applied a risk adjustment of 10%, yielding a three-year, risk-adjusted total PV of $321,524.

Avoided Cost Of Ransomware Attacks: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
B1	Annual revenue	5% YoY growth	$230,000,000	$241,500,000	$253,575,000
B2	Daily revenue	B1/260	$884,615	$928,846	$975,288
B3	Percentage of critical projects impacted	Assumption	5%	5%	5%
B4	Time to restore file access (days)	Interviews	5	5	5
B5	Potential business impact of a ransomware attack	B2*B3*B4	$221,154	$232,212	$243,822
B6	Cost of post-attack assessment and administration (HR, legal, IT operations, executive time)	Estimate	$50,000	$50,000	$50,000
B7	Probability of ransomware attack	Ponemon Institute	51%	51%	51%
Bt	Avoided cost of ransomware attacks	(B5+B6)*B7	$138,288	$143,927	$149,849
	Risk adjustment	↓10%	.		
Btr	Avoided cost of ransomware attacks (risk-adjusted)		$124,460	$129,535	$134,864

Avoided Costs For Alternative Solution

The Acronis Cyber Protection solution enabled the interviewed organization to back up and secure its data at a substantially lower cost than scaling up its use of a preexisting cloud storage solution.

Prior to implementing the Acronis Cyber Protection solution, the interviewed organization backed up its business data using magnetic tape storage and capacity from a public cloud vendor. Magnetic tapes were inexpensive to procure, but backing up data this way was time-consuming and inefficient. Leveraging the public cloud solution was seamless, but the organization only had access to 1 petabyte (PB) of storage, and scaling up its usage of this solution would have been costly.

The interviewed organization procured a total of 4.5 million GBs of storage capacity from Acronis to ensure that it could back up the quickly growing volume of data being generated by the business. To procure the same amount of capacity from a public cloud storage vendor, the organization would have paid about 50% more.

The following assumptions are represented in the financial model for this benefit category:

- The organization completely retires its tape backup solution when it switches to cloud-only backup, producing a one-time savings of $50,000 on annual maintenance fees.
- If the organization chose to back up its data with its preexisting cloud storage solution provider, its annual costs would have depended on the type of data stored and how frequently it needed to access that data: 65% of the organization's data would have been appropriate for low-cost, archive-tier storage; 35% of the organization's data would have required hot or file-tier storage.
- Monthly per GB costs for data storage are inclusive of egress and other fees.

The following factors may also contribute to variability in the impact of this benefit category:

- The amount of capacity used versus capacity owned, which will impact the cost savings realized with Acronis. For example, if the organization does not utilize all of the capacity purchased from Acronis, it may not realize a true cost savings, since it may pay less with a consumption-based plan.
- Changes over time in the cost of storing data with public cloud storage solution providers.
- Changes over time in the composition of the organization's data set — e.g., the percentage of data that is suitable for archive-tier storage.

To account for this variability, Forrester applied a risk adjustment of 5%, yielding a three-year, risk-adjusted total PV of $7,570,137.

The interviewed organization procured a total of 4.5 million GBs of storage capacity from Acronis to ensure that it could back up the quickly growing volume of data being generated by the business. To procure the same amount of capacity from a public cloud storage vendor, the organization would have paid about 50% more.

FORRESTER®

Avoided Costs For Alternative Solution: Calculation Table					
REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
C1	Avoided maintenance costs for tape storage solution		$50,000		
C2	Backup storage (GB)		4,500,000	4,500,000	4,500,000
C3	**Percentage: archive**		**65%**	**65%**	**65%**
C4	**Percentage: hot**		**20%**	**20%**	**20%**
C5	**Percentage: file**		**15%**	**15%**	**15%**
C6	**Storage tier: archive (GB/month)**		**$0.01**	**$0.01**	**$0.01**
C7	**Storage tier: hot (GB/month)**		**$0.15**	**$0.15**	**$0.15**
C8	**Storage tier: file (GB/month)**		**$0.15**	**$0.15**	**$0.15**
C9	**Storage cost: archive**	**C2*C3*C6*12**	**$351,000**	**$351,000**	**$351,000**
C10	**Storage cost: hot**	**C2*C4*C7*12**	**$1,620,000**	**$1,620,000**	**$1,620,000**
C11	**Storage cost: file**	**C2*C5*C8*12**	**$1,215,000**	**$1,215,000**	**$1,215,000**
Ct	Avoided costs for alternative solution	C1+C9+C10+ C11	$3,236,000	$3,186,000	$3,186,000
	Risk adjustment	↓5%			
Ctr	Avoided costs for alternative solution (risk-adjusted)		$3,074,200	$3,026,700	$3,026,700

Unquantified Benefits

› **Avoidance of extreme business disruption and reputational damage.** The financial benefits section of this study estimates the avoided cost of small-scale business disruption associated with a potential ransomware attack. However, this study doesn't attempt to quantify the avoided cost of significant disruption to business operations (e.g., the inability to deliver a product on schedule) or the loss of key customer accounts due to a loss in trust. However, costs that reach tens or hundreds of millions of dollars aren't unheard of for enterprises that encounter ransomware attacks. Merck, for example, reported costs associated with the NotPetya ransomware attack at approximately $670 million.[7] The same year, FedEx reported losses of $300 million in its first-quarter earnings release, which it attributed to NotPetya.[8]

A ransomware attack could have a potentially catastrophic impact on the business if its data was lost or exposed.

- **More comprehensive data backups, which provide employees with access to data they need to do their jobs.** Prior to adopting the Acronis Cyber Protection solution, it could take IT operations staff days to fulfill a data recovery request, leaving employees without data essential to move projects forward. In some cases, data couldn't be recovered at all, because either 1) the data wasn't backed up in the first place or 2) the data was routinely discarded after a set period of time due to storage limits. The Acronis Cyber Protection solution enables the organization to more thoroughly back up its data and restore files promptly upon request. However, the impact on productivity of having access to complete file histories is difficult to quantify and is not represented in the financial benefits section of this analysis.
- **Better organizational resilience.** In the event that one of the organization's data centers goes offline, Acronis enables IT staff to replicate it in a matter of hours. The interviewed organization has two onsite data centers. In the event that one goes down, it can restore everything stored in the failed environment to the one that's fully functioning, ensuring that critical systems are available to the business. According to the chief information officer, the organization lacked these capabilities in the past, and it was vulnerable to disruption in operations.

Analysis Of Costs

QUANTIFIED COST DATA

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Dtr	Fees paid to Acronis	$350,000	$2,050,000	$2,050,000	$2,050,000	$6,500,000	$5,448,047
Etr	Setup and implementation costs	$5,077	$0	$0	$0	$5,077	$5,077
	Total costs (risk-adjusted)	$355,077	$2,050,000	$2,050,000	$2,050,000	$6,505,077	$5,453,124

Fees Paid To Acronis

The interviewed organization paid one-time fees to Acronis for professional services and implementation support. It also pays ongoing fees for hybrid cloud storage capacity and access to Acronis data protection solutions.

Acronis provided upfront and ongoing costs, and Forrester confirmed these costs with the customer. Therefore, Forrester applied no risk adjustment to this category. Three-year costs for professional services, capacity, and ongoing access to Acronis data protection solutions total $5,448,047 in present value.

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 interviewed organization expects risk-adjusted total costs to be a PV of more than $5.4 million.

Fees Paid To Acronis: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
D1	Professional services fees paid to Acronis		$350,000			
D2	Ongoing cloud backup and support fees			$2,050,000	$2,050,000	$2,050,000
Dt	Fees paid to Acronis	D1+D2	$350,000	$2,050,000	$2,050,000	$2,050,000
	Risk adjustment	0%				
Dtr	Fees paid to Acronis (risk-adjusted)		$350,000	$2,050,000	$2,050,000	$2,050,000

FORRESTER®

Setup And Implementation Costs

To a large extent, Acronis' professional services team oversaw the setup and implementation process, and these costs are reflected in the section titled Fees Paid To Acronis. However, the interviewed organization did incur nominal costs for time spent on planning, implementation, and training activities over the course of 12 weeks.

The financial model for this cost category shows the following:

- One member of the organization's IT operations staff spent 12 weeks conducting a comprehensive audit of the business' databases, applications, and servers. (The results of this analysis were handed over to Acronis prior to the professional services team starting on the implementation.) During that time, the project leader spent 15% of each week's working hours on audit-related activities.
- Two members of the organization's IT operations staff received formal training on the Acronis solution from the Acronis professional services team. The training session lasted three days (or 0.6 weeks, as shown in the table below).

Forrester risk-adjusted setup and implementation costs upward by 10% to account for factors variability in results that organizations may experience as a result of the following:

- The number of databases, applications, and servers under management, which may increase the amount of time required to complete a comprehensive audit.
- The number of IT operations staff members that require training.

This adjustment yielded a three-year PV total cost of $5,077.

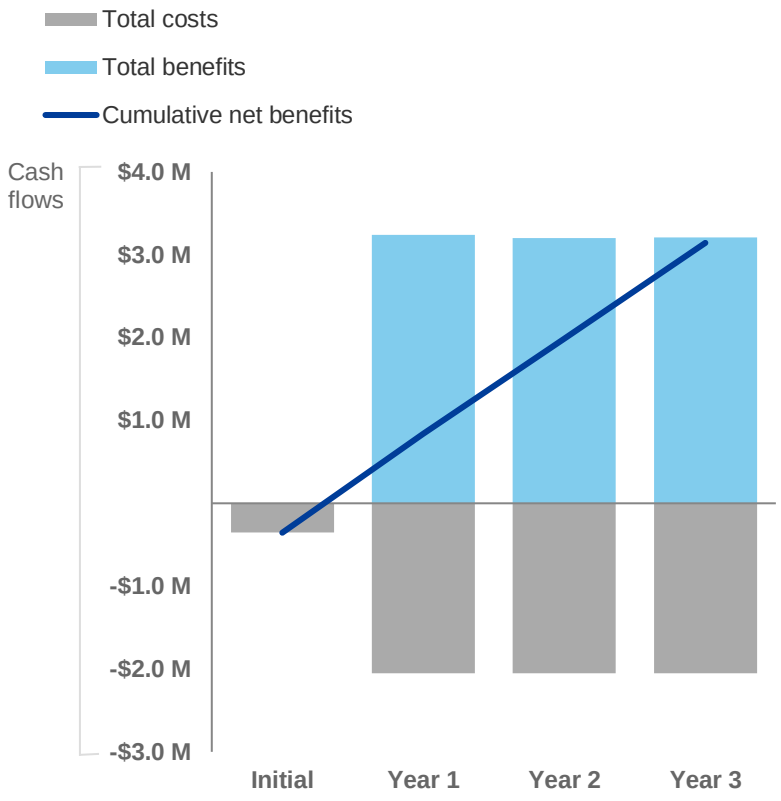
Implementation risk is the risk that a proposed investment may deviate from the original or expected requirements, resulting in higher costs than anticipated. The greater the uncertainty, the wider the potential range of outcomes for cost estimates.

Setup And Implementation Costs: Calculation Table						
REF.	**METRIC**	**CALC.**	**INITIAL**	**YEAR 1**	**YEAR 2**	**YEAR 3**
E1	Weeks required for planning (audit of applications and servers)		12			
E2	IT operations analysts involved in planning phase of project		1			
E3	Percentage of time spent on planning activities		15%			
E4	Total hours dedicated to planning activities	E1*E2*E3*40	72			
E5	Weeks required for training		0.6			
E6	IT operations analysts involved in training sessions		2			
E7	Percentage of time spent on training activities during training period		100%			
E8	Total hours dedicated to training sessions	E5*E6*E7*40	48			
E9	IT operations analyst hourly rate, fully burdened		$38.49			
Et	Setup and implementation costs	(E4+E8)*E9	$4,615	$0	$0	$0
	Risk adjustment	↑10%				
Etr	Setup and implementation costs (risk-adjusted)		$5,077	$0	$0	$0

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 interviewed 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	($355,077)	($2,050,000)	($2,050,000)	($2,050,000)	($6,505,077)	($5,453,124)
Total benefits	$0	$3,241,410	$3,200,268	$3,206,918	$9,648,595	$8,000,990
Net benefits	($355,077)	$1,191,410	$1,150,268	$1,156,918	$3,143,518	$2,547,866
ROI						47%
Payback period						< 6 months

FORRESTER®

Acronis Cyber Protection: Overview

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

Acronis Backup delivers the data protection that meets the demands of today's modern IT infrastructure from mission-critical data center workloads to edge devices. Our solutions provide complete protection — Cyber Protection — in an unparalleled manner that includes each of the following five vectors of protection:

- **Safety** — A copy of data for recovery.
- **Accessibility** — Ability to access the data.
- **Privacy** — Control over access to data.
- **Authenticity** — Ability to verify origins of data.
- **Security** — Protection from cyberthreats.

Acronis' mission is to deliver Cyber Protection in an easy, efficient, and secure way, providing reliability and full control for the enterprise. Acronis' solutions are trusted by over 500,000 businesses, including 79 of the top 100 most valuable brands. Acronis' products are available through 50,000 partners and service providers in over 150 countries in more than 25 languages.

Acronis Active Protection Harnesses Artificial Intelligence For Anti-ransomware And Cryptojacking

Acronis Active Protection is an advanced ransomware protection technology. Compatible with the most common antimalware solutions, Acronis' technology actively protects all of the data on your systems, including documents, media files, programs, and even Acronis Backup Files. Acronis Active Protection uses artificial intelligence (AI) to constantly observe patterns in how data files are being changed on a system. One set of behaviors may be typical and expected. Another set of behaviors may signal a suspect process taking hostile action against files. The Acronis AI looks at these actions and compares them against malicious behavior patterns. This approach can be exceptionally powerful in identifying attacks, even from ransomware variants or cryptojacking approaches that are as-yet unreported. Once a malicious behavior is identified, the Acronis Active Protection immediately shuts down the malicious processes and triggers a recovery of any affected or encrypted files from backup.

Acronis Cyber Services and AI Consulting

Acronis also offers a range of professional services and consulting to help its customers with Cyber Protection and AI design and implementation.

- **Security Assessment Services.** These include risk assessment, vulnerability scanning, penetration testing of the network, web and mobile applications, and social engineering. The result is a detailed report of findings and mitigation recommendations.
- **Security Awareness Services.** These include training modules for different user levels, including modules to address governance and audit requirements. The result is a management report and dashboard outlining an organization's security posture.
- **Incident Response Services.** These include security breach diagnostics, consultation and recommended responses. The result is a detailed report about the event(s) and mitigation recommendations.
- **AI Consulting Services.** These professional services are being taken advantage of by key Acronis sports partners to apply AI to the massive amounts of data being stored to develop unique competitive advantages. One such partner is NIO, a Formula E race team, which has engaged Acronis AI Consulting Services for sensor failure detection, video analytics of races, and a live strategy tool for in-race decision making.

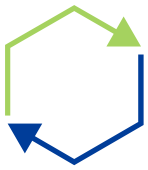
Appendix A: Total Economic Impact

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

Total Economic Impact Approach

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

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



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

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

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

Present value (PV)

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

Net present value (NPV)

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

Return on investment (ROI)

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

Discount rate

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

Payback period

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

Appendix B: Endnotes

[1] Source: “Ransomware Is A Business Continuity Issue,” Forrester Research, Inc., May 22, 2018.
[2] Source: Nash, Kim S., “One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs,” The Wall Street Journal, June 27, 2018 (https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906).
[3] Source: Forrester Analytics Global IT Business Continuity And Disaster Recovery Preparedness Online Survey, 2017
[4] Source: Nash, Kim S., “One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs,” The Wall Street Journal, June 27, 2018.
[5] Source: Johnson, Eric M., “Cyber attack, hurricane weigh on FedEx quarterly profit,” Reuters, September 19, 2017 (https://www.reuters.com/article/us-fedex-results/cyber-attack-hurricane-weigh-on-fedex-quarterly-profit-idUSKCN1BU2RG).
[6] Source: “The Rise Of Ransomware,” The Ponemon Institute, January 17, 2017 (https://www.ponemon.org/local/upload/file/Ransomware%20Report%20Final%201.pdf).
[7] Ibid
[8] Source: Johnson, Eric M., “Cyber attack, hurricane weigh on FedEx quarterly profit,” Reuters, September 19, 2017 (https://www.reuters.com/article/us-fedex-results/cyber-attack-hurricane-weigh-on-fedex-quarterly-profit-idUSKCN1BU2RG).