ROI REPORT
TAYLOR COMMUNICATIONS

Determining ROI for ReliaTech's Cyber Recovery Unit

An ROI Report™ by Taylor Communications

Table of Contents

Abstract

Unplanned system downtime, such as an outage caused by a ransomware attack, leads to unexpected costs. There is the expense of paying for idle employees and facilities, as well as the opportunity cost of lost profits when systems are down. ReliaTech offers a failover solution that reduces unplanned downtime—along with the associated costs.

This paper examines how ReliaTech's ability to shrink unplanned downtime translates into return on investment (ROI) for the technology. It uses the example of a hypothetical mid-sized business to model the financial impact of ReliaTech's solution on the company's operations, income, and expenses.

Introduction

If there were a prize for the most unpopular phrase in the business world, "Our systems are down" would be a top contender. No one wants to hear these words, from frustrated customers to stressed-out employees. The C-suite doesn't want to hear the phrase either, because unplanned downtime is expensive in more ways than one. Not only does a company lose revenue when its systems are down, it's also paying people to sit around and do nothing.

A solution like ReliaTech's Cyber Recovery Unit (CRU), which can reduce unplanned downtime, delivers financial value along with technology benefits. An investment in ReliaTech's CRU will bring returns—a return on investment (ROI).

This paper explores how the ReliaTech solution generates ROI for companies that invest in it. Using operational estimates and data from industry research, it models the factors that contribute to ROI. These include lower expenses arising from unplanned downtime incidents, reductions in lost operating time, less revenue lost, and more.

The ROI estimates shown in this paper are based on ReliaTech's ROI calculator, which can be downloaded for customized analysis *here*.

Understanding the Problems that ReliaTech Solves

It's not big news that computer systems are under attack. What we seem to have missed amid the onslaught of ransomware attacks and myriad other threats is how our assumptions about risk have taken shape. Many of us simply assume that we're going to be attacked, and when that happens, we'll be dealing with a costly, time-consuming cybersecurity incident and some unpredictable amount of unplanned downtime.

It's worth questioning this assumption. Unplanned downtime, the scourge of *"our systems are down...please bear with us..."* is not a given. It's the result of systemic weaknesses that can be addressed with innovative technology. This is the problem that ReliaTech solves.

Air-gapped, each CRU stores an instantly retrievable backup copy of critical, timely data for rapid restoration.

ReliaTech offers failover solutions for cyber resilience that reduce, or even eliminate unplanned downtime. These solutions achieve this goal through the use of proprietary CRUs. These hardware-based appliances attach to devices at risk for unplanned downtime. Air-gapped, each CRU stores an instantly retrievable backup copy of critical, timely data for rapid restoration. In most cases, it only takes 30 seconds to return a system back to work when there is a cyberattack or systemic malfunction.

The CRU can protect information technology (IT) systems as well as operational technology (OT) devices. This latter category includes industrial control systems, building management systems, and the like. OT tends to be more vulnerable to attack than IT, partly because OT relies on older technology that has not kept up with cyber risk mitigation practices and updates. By protecting both IT and OT, ReliaTech minimizes the impact of unexpected systems outages.

Identifying the Return on a Technology Investment

ROI can mean different things to different people, so it's worth taking a moment to share how we define the concept. Most of us intuitively get the idea of ROI. If we buy a stock that pays a dividend, the dividend is the return on the investment.

ROI can be captured by the following simple equation:
ROI = R ÷ I

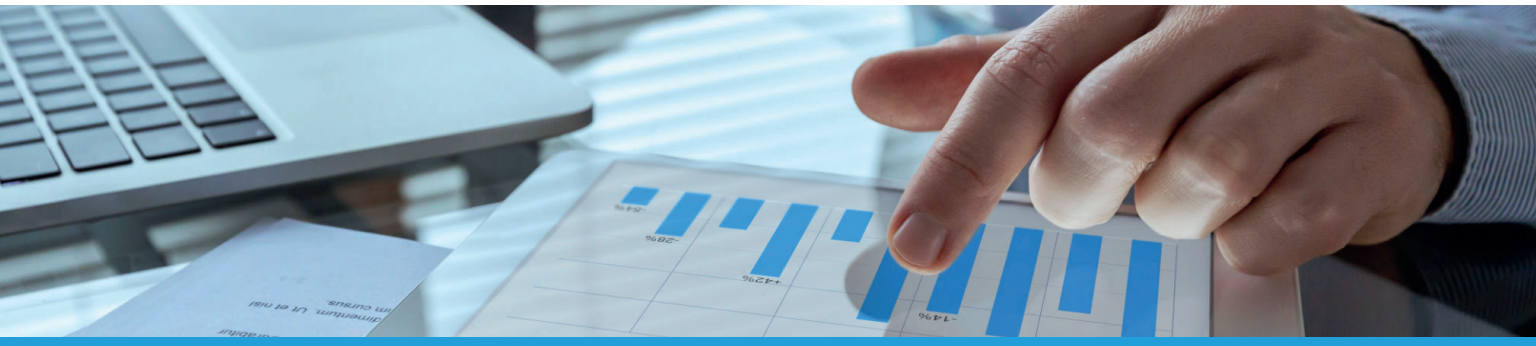
So, if you paid $100 for a share of stock and earned a $10 dividend, your "I" = $100 and your "R" = $10. **ROI is $10/$100 or 10%.**

Investing in technology is not that different. If you purchase a technology solution for $1 million, your "I" is $1 million. The question is, "What is the 'R'?" That's where things can get a little complicated, but in most cases, any savings or increases in earnings resulting from the investment constitute your "R." If you saved $50,000 by investing $1 million in a solution, your ROI is $50,000/$1,000,000, or 5%.

ROI may be a onetime estimate, or ongoing. If the $1 million investment saves $50,000 per year, then the ROI is 5% per year.

For our purposes, ROI comes from calculations involving tangible numbers based on reasonable assumptions. It's not that intangible returns are unimportant. Indeed, factors like reputation and brand value can be extremely relevant to the procurement decision making process.

The problem is that they are difficult to estimate with any accuracy. Intangibles also tend not to be persuasive to the people who sign checks.



Why ROI Matters

Business leaders may insist on an ROI analysis before spending money. They do this for several reasons, most of which have to do with earnings.

Corporate managers are almost always driven—and compensated—by growth in share price. If an investor bought a share for $10 last year, and now it's worth $12, that $2 gain in price is the investor's ROI. Investors in private companies have the same perspective.

How will managers achieve that $2 gain in share price? One way is to earn ROI on the company's most important asset, its cash.

In other words, managers are also under pressure to demonstrate ROI for their spending of the shareholders money. Good managers will therefore require that any investment of the company's cash must generate an ROI.

On a related front, companies often borrow money to invest in IT solutions. That solution should ideally generate an ROI higher than the interest on the borrowed money. If the company borrowed at 7% interest, then it will want to invest that money for a return greater than 7%.

For these reasons, an ROI estimate is typically expected for an IT investment or expense.

Drivers of ROI for ReliaTech Failover Solutions

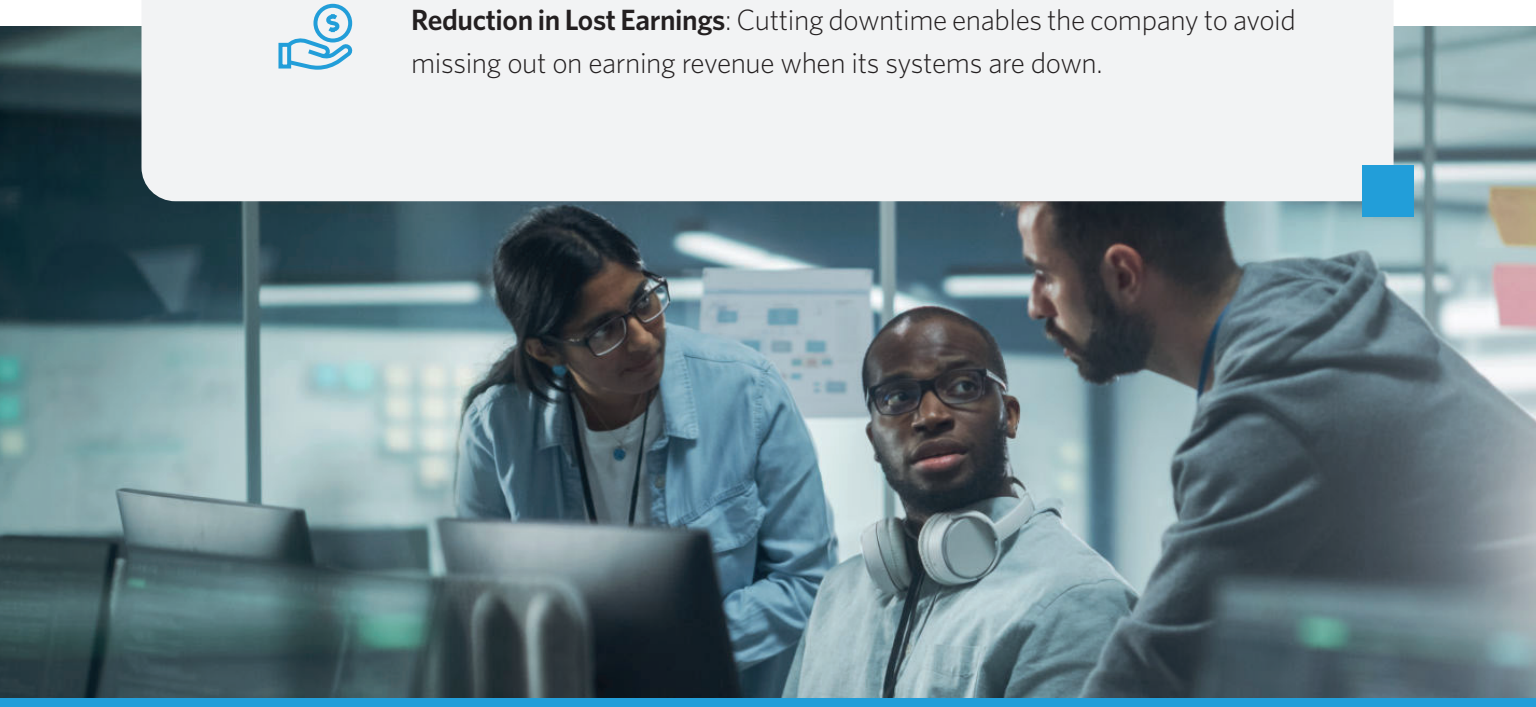
ReliaTech's solution generates ROI from cost savings and revenue/earnings increases:

Less Unplanned Downtime: Every minute that systems are down, costly assets, as well as employees, are idle. The company wastes money. If the business could avoid paying people and machines to do nothing, its earnings would be higher.

Fewer Incidents: Cybersecurity incidents, such as ransomware attacks, can be expensive to remediate. Outlays for dealing with an incident run the gamut from IT consultants, forensics, legal fees, PR firms, overtime, customer notifications, and more. ReliaTech's solution reduces the number of unplanned downtime incidents that a company will face, which saves money.

Lower Expenditures on Security: With an effective failover solution in place, the company can reduce its cybersecurity budget.

Reduction in Lost Earnings: Cutting downtime enables the company to avoid missing out on earning revenue when its systems are down.



ROI Analysis

Determining ROI is a process that requires establishing facts about a business and making assumptions about how a given technology will affect that business. For the purposes of this paper, we are going to use the example of ZCorp, a hypothetical mid-sized business. The ROI analysis for ReliaTech's impact on ZCorp starts with the following basic facts about the business:

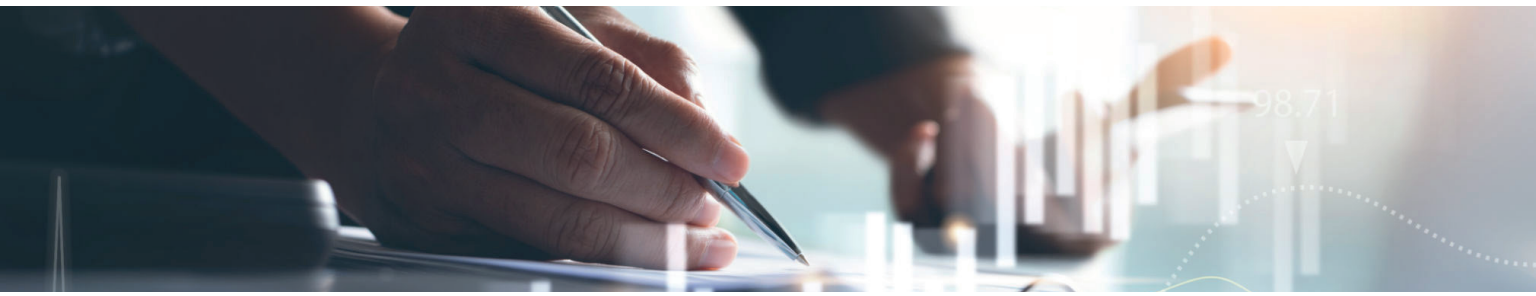
ZCorp Basics	
Annual Revenue	**$65,000,000**
Annual cost of operations	**$30,000,000**
Hours of operation per week	**50**
Weeks of operation per year	**50**
Total hours of operation per year	**2,500**

ZCorp operates for 2,500 hours per year. Before the investment in ReliaTech's technology, the company had a 99% rate of uptime, meaning that 1% of operating time, 25 hours per year, was unplanned downtime. Based on ReliaTech's experience with clients of this size, its technology can deliver a 50% reduction in unplanned downtime. ZCorp will then have an uptime rate of 99.5%, which translates into 12.5 hours of downtime per year.

The investment will enable the company to reduce unplanned downtime from 25 hours to 12.5.

The investment will enable the company to reduce unplanned downtime from 25 hours to 12.5. That estimated drop in unplanned downtime is a critical piece of information for making ROI calculations.

Rates of Unplanned Downtime	
Current uptime rate	**99.00%**
Current rate of unplanned downtime	**1.00%**
Current number of hours of unplanned downtime per year	**25**
Reduction in unplanned downtime resulting from investment in technology	**50%**
Projected rate of uptime after investment	**99.50%**
Projected hours of unplanned downtime avoided per year after investment	**12.5**



Operational Cost Savings

How will cutting unplanned downtime affect ZCorp's operational costs? Given that the company has an annual cost of operations of $30 million, and operates for 2,500 hours per year, we can conclude that each hour of operations costs ZCorp $12,000.

The pre-investment amount of unplanned downtime, 25 hours, translates into a cost of $300,000, as the chart below demonstrates (25 hours x $12,000 per hour). With ReliaTech, ZCorp cuts its downtime to 12.5 hours, so after the technology investment, it has reduced its downtime cost to $150,000 (12.5 hours x $12,000 per hour).

Operational Cost Savings	
Annual cost of operations	**$30,000,000**
Hours of operation per year	**2,500**
Cost of operations, per hour	**$12,000**
Current cost of unplanned downtime (cost of operations)	**$300,000**
Projected cost of unplanned downtime after investment	**$150,000**
Savings in cost of unplanned downtime	**$150,000**

Incident Response Savings

Responding to a cybersecurity incident can be a costly undertaking. IBM research estimates that a large enterprise can spend upwards of $1.2 million dealing with the aftermath of a cyberattack and resulting outages. For ZCorp, which is a medium-sized company, we'll estimate its cost for an incident at $250,000. Then, based on ReliaTech's experience working with similar clients, we will project that the use of ReliaTech's solution will lead to ZCorp experiencing one incident per year versus two. As a result, as shown in the table below, ZCorp's cost for incident response drops from $500,000 per year to $250,000 after making the investment in the ReliaTech solution.

Change in Incident Response Costs	
Current number of unplanned downtime incidents per year	**2**
Projected change in number of unplanned downtime incidents	**-50%**
Projected number of unplanned downtime incidents	**1**
Incident response costs - per incident (system recovery, consultants, legal, etc.)	**$250,000**
Current cost of unplanned downtime incidents	**$500,000**
Projected cost of unplanned downtime incidents after investment	**$250,000**
Savings in incident response costs	**$250,000**

Reduced Opportunity Costs

When ZCorp's systems are down, it can't make any sales. This is known as the opportunity cost of unplanned downtime. With revenue of $65 million and 2,500 operating hours per year—and a gross margin of 60%—ZCorp is generating gross profit at the rate of $15,600 per hour. We use gross profit as the metric for opportunity costs instead of revenue because gross profit represents actual income from operations.

Opportunity Costs of Unplanned Downtime	
Total revenue from annual production	**$65,000,000**
Gross margin	**60%**
Gross profit earned per hour of operations	**$15,600**
Current gross profit losses due to unplanned downtime	**$390,000**
Projected gross profit losses due to unplanned downtime after investment	**$195,000**
Delta in gross profit losses due to unplanned downtime	**$195,000**

Pre-investment, ZCorp was missing out on $390,000 in gross profits (25 hours per year x $15,600 per hour). After the investment in ReliaTech's solution, ZCorp will have opportunity costs from unplanned downtime of $195,000 (12.5 hours per year x $15,600 per hour). The change amounts to a net gain in gross profits of $195,000.

Adding the hourly operational cost of unplanned downtime ($12,000) to the hourly opportunity cost ($15,600), we get a total hourly cost of unplanned downtime of $27,600. This number falls into the range of industry averages calculated by Solar Winds, which is between $25,000 for a small business and $540,000 for a large enterprise.

Reduced Spending on Cybersecurity

In ReliaTech's experience, use of its solution generally leads to a reduction in spending on cybersecurity. ZCorp will not need as many cybersecurity resources to address vulnerabilities and threats if it can count on rapid failover and recovery. We will estimate ZCorp's cybersecurity budget at 10% of their $520,000 overall IT budget. These estimates are based on industry research on *IT* and *cybersecurity expenditures* as a percent of revenue. Based on ReliaTech's work with comparable clients, we project that use of the ReliaTech solution will enable ZCorp to save 10% on its cybersecurity budget, or $52,000 per year.

Reductions in Cybersecurity Spending	
Overall IT budget	**$5,200,000**
Cybersecurity budget as % of IT spend	**10%**
Cybersecurity budget	**$520,000**
Reduction in cybersecurity spending	**10%**
Savings in cybersecurity spending	**$52,000**

Overall ROI Calculation

The savings and changes in gross profit brought about by the ReliaTech solution total $647,000, as shown in the chart below. This the "R" in our ROI calculation. The investment, or "I," is $1 million. The annual ROI is therefore 65%. (Note: ROI in subsequent years may be lower, because the savings in cybersecurity spending may not recur.)

Overall ROI Calculation	
Operational savings from change in cost of unplanned downtime	**$150,000**
Savings in incident response costs	**$250,000**
Delta in gross profit losses due to unplanned downtime	**$195,000**
Savings in cybersecurity spending	**$52,000**
Total annual cost and revenue impact of investment	**$647,000**
Investment in technology	**$1,000,000**
Return on investment (ROI)	**65%**

Takeaways and "What Ifs"

Getting to an ROI estimate is a subjective process that relies on many assumptions about how a technology will affect operational realities. However, an investment in a technology will always deliver a return of some kind. It may be low, or even be negative, with the technology costing more than it returns in savings and revenue.

A good practice is to think through your assumptions and model ROI for multiple scenarios. This process will yield a range of possible ROI outcomes. For example, if we posit that ReliaTech's solution will result in a 75% reduction in unplanned downtime, instead of 50%, the ROI increases to 82%. Similarly, if we exclude the reduction in unplanned downtime incidents from the calculation, ROI drops from 65% to 40%.

Working this way, we can use the formula to build a chart that shows the impact of different uptime assumptions on ROI:

What If? ROI Scenarios Modeled for Different Changes in Rates of Unplanned Downtime

Change in unplanned downtime	10%	20%	30%	40%	50%	60%	70%	80%	90%
ROI	$371,000	$440,000	$509,000	$578,000	$647,000	$716,000	$785,000	$854,000	$923,000
ROI %	37%	44%	51%	58%	65%	72%	79%	85%	92%

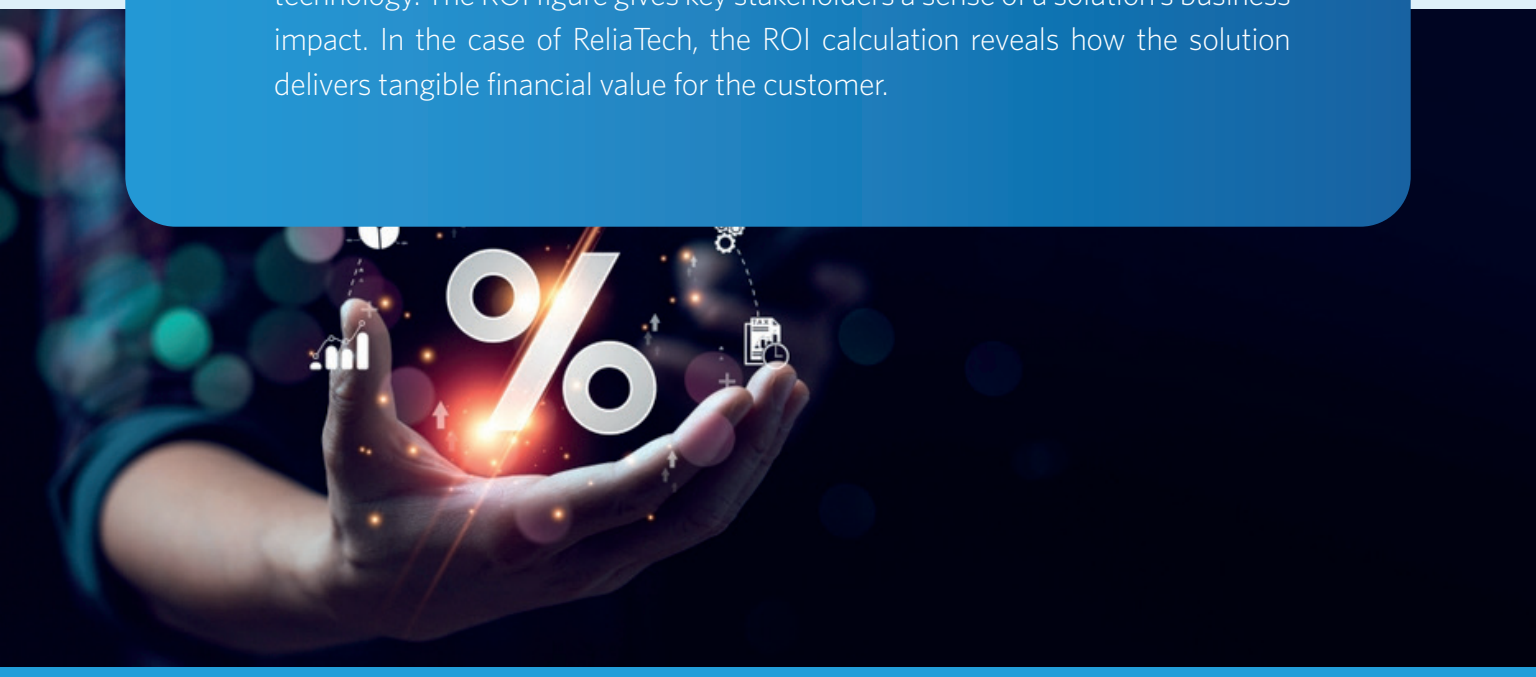
A range of ROI outcomes like the one shown in the chart can be useful for exploring ROI from alternative points of view, such as, "What kind of reduction in unplanned downtime do we need to achieve to make this investment worthwhile?"

Conclusion

Unplanned downtime is a disruptive, costly problem for virtually every company. Some amount of unplanned downtime is probably inevitable, but it is possible to mitigate its impact with solutions like ReliaTech's CRU. By reducing unplanned downtime with rapid failover and recovery of IT assets, ReliaTech enables customers to reduce expenses that arise from stalled operations and incident response. The solution also cuts down on the opportunity cost of lost profits from unplanned downtime.

These factors, together with reductions in cybersecurity spending, make it possible to estimate ROI for the ReliaTech solution. Using the ROI calculation methods shared in this paper, it is possible to project, for example, that a 50% improvement in unplanned downtime will result in an ROI of 65%.

Determining ROI should be an essential part of deciding whether to invest in a technology. The ROI figure gives key stakeholders a sense of a solution's business impact. In the case of ReliaTech, the ROI calculation reveals how the solution delivers tangible financial value for the customer.



About the ROI Report

The ROI Report™ from Taylor Communications leverages technology analyst Hugh Taylor's proprietary methodology to demonstrate the potential return on investment (ROI) for a technology solution. It is based on Taylor's experience training account teams at IBM in consultative selling.

Taylor is a technology analyst and writer with more than two decades of experience in evaluating the business value of technology investments. He has demonstrated proven expertise in technology analysis and marketing communications for clients in cloud computing, security, collaboration tools, software development tools, social computing, and enterprise architecture.

ROI REPORT

TAYLOR COMMUNICATIONS

An ROI Report™ by Taylor Communications