Optimize Risk, Value and Cost in Cybersecurity and Technology Risk

By Paul Proctor
Optimize Risk, Value and Cost in Cybersecurity and Technology Risk

Cybersecurity should balance the needs to protect against the needs to achieve desired business outcomes. CIOs can attain this balance by optimizing risk and value in a business context through the lens of key stakeholder needs.

Overview

Key Challenges

- CIOs, executives and boards of directors struggle to know how much cybersecurity is enough.
- Cybersecurity is often treated as a siloed issue managed by technology experts and best addressed by a compliance approach where “more” is always seen as better.

Recommendations

CIOs seeking to optimize IT risk and corporate performance should:

- Optimize cybersecurity risk in a business context through the lens of stakeholder needs to drive decisions related to prioritization and investments.
- Sharpen their ability to understand and communicate a business context around technology and the business outcomes they support.
- Balance cybersecurity investment and risk with the needs to achieve desired business outcomes.
- Integrate risk, value and cost optimization into cybersecurity business cases, committee reviews, funding requests and board reporting.
Introduction

Optimizing cybersecurity risk in a business context through the lens of stakeholders needs creates a powerful model to drive decisions related to prioritization and investments. It is particularly useful in developing and presenting cybersecurity business cases, committee reviews, funding requests and board reporting. Risk-optimized decisions will help an organization settle on how much security is enough for their circumstances.

Risk, value and cost (RVC) optimization demonstrates to key stakeholders like shareholders, customers, regulators and partners that the organization has the right priorities and investments to create a balance between the needs to address risk with the needs to achieve their desired business outcomes.

A risk-optimized approach creates credibility and defensibility that an organization is appropriately protected whether they have experienced a material cybersecurity incident or not.

A risk, value and cost optimization decision model guides decision making that optimizes cybersecurity in a business context through the lens of key stakeholder needs.
Analysis

Optimize Cybersecurity Priorities and Investments for Risk, Value and Cost

Risk-Optimized Cybersecurity Decisions. A cybersecurity priority or investment decision is considered optimized for risk, when it has the following characteristics:

- A conscious business decision is made related to priorities and investments, in a business context.
- The decisions have credibility and defensibility with key stakeholders.
- Informed by:
  - Known levels of cybersecurity risk in a business context.
  - Choices to address known cybersecurity risk in a business context.
  - Key stakeholder needs related to relative cybersecurity risks in a business context.

All cybersecurity decisions result in residual risk because there is no such thing as perfect protection. And the level of that risk is ultimately a choice related to investments and priorities.

When we plot business units by their value against their readiness to address known risks, and include consideration of cost, we are presented with a comparative analysis that supports priority and investment decisions in a business context (see Figure 1).
The optimized risk zone is a reflection that higher risk is more credible and defensible when value is low. When value is high, then lower risk is necessary to be credible and defensible through a stakeholder lens. Treating risk generally increases cost and the inclusion of cost also supports business decision making.

For example, a choice to continually underinvest in cybersecurity to keep IT costs lower does not optimize risk. This may lower costs, but with full visibility into the risk of a major cybersecurity incident, like a ransomware attack or a headlining breach, this may not be an acceptable position for the shareholders, customers or partners.

Risk and security capabilities are often presented in an enterprisewide context that does not have sufficient business context to optimize risk and balance the needs to protect with the needs to run the business. By assessing the performance of risk and security controls in the context of the infrastructure and parts of the application portfolio that support each business unit or operating unit, we can better guide priorities and investments in a business context.

The level of cybersecurity risk experienced by each business unit is plotted against business value. We can now optimize risk in a business context through the lens of stakeholder credibility and defensibility:
Examples where cybersecurity RVC optimization delivers value:

- **Business Unit A** is very business-critical (contributes 30% of top-line revenue, in a regulated industry, has a lot of personally identifiable information [PII]) but poor cybersecurity capabilities. This is likely not credible and defensible with shareholders and regulators so priorities and investments should be made to improve cybersecurity capabilities.

- **Business Unit B** has lower business criticality and commensurately less need for high cybersecurity capabilities (no PII, less sensitivity to unscheduled outage) so it may be credible and defensible to have higher cybersecurity risks and lower investments in addressing it.

- **Business Unit E** has high business criticality with commensurate levels of investment to create good cybersecurity capabilities within acceptable levels for shareholders and regulators.

- **Business Unit F** has low business criticality, but higher levels of investment to create world-class cybersecurity capabilities. It may be appropriate for the CFO to suggest that Business Unit F has overinvested in the latest technology advances to maintain an unnecessary level of cybersecurity protection.

Examples where cybersecurity RVC optimization delivers value:

- How much should we spend on cybersecurity?
- How can we manage cybersecurity risk with our partners?
- What are the right priorities and investments in cybersecurity technology?

There are a number of factors that influence the credibility and defensibility of the assessment and decisions that are made, as described below. Ultimately, the model is about using the relationship between risks, value and cost so that credible and defensible business decisions can be made that optimize risk.

From these observations, a prioritized plan of investments can be recommended to negotiate an action plan to bring all the business units in line with optimized risk.

**Risk is ultimately a choice related to investments and priorities.**
The RVC Optimization Decision Model for Cybersecurity

The Gartner RVC optimization model assesses four primary constructs: risk, cost, value and targets. There are three primary lenses: stakeholder credibility and defensibility, business context and the risk optimization zone. Plotting assessment targets in the model supports risk optimized decision making (see "A Decision Model to Optimize Risk, Value and Cost").

Assessment Targets in Cybersecurity

A variety of targets can be plotted on the RVC optimization model to support decision making, including initiatives, business processes, projects and business units. The comparative nature of the model shows risks of each target relative to the others which highlights outliers and promotes prioritization and investment decisions. Figure 1 shows the targets as the stars of different sizes, plotted across the dimensions of value and risk.

- **Which business outcomes are at cybersecurity risk?** Identify the business operating capabilities that deliver value and are at risk to facilitate business decisions made in a business context.

**The Value Dimension**

Value should influence risk and investment considerations. Figure 1 presents value as the vertical (y-axis) with low value on the bottom and high value on the top.

- **What is the value of the business outcomes?** Value can be measured by level of investments, expected business outcomes, revenue or other measure that represents size, scope or breadth of the targets that are being assessed for RVC optimization.

Value should be discussed and agreed to by executives to support decision making and engagement.

**The Risk Dimension**

It is a business decision to choose any level of risk. Figure 1 presents risk as the horizontal (x-axis) from lower risk on the left to higher risk on the right. Risk can be assessed in any meaningful, content-dependent manner.

- **How much risk is acceptable?** Risk levels can be treated and changed through dedicated investments (cost) specifically designed to address known risks.
Risk for cybersecurity should be measured as a function of control readiness to address identified threats, not the risk of the threats themselves. For example, it is not effective to measure the risk of ransomware because you do not control ransomware. You do, however, control your investments in the mechanisms that address ransomware — such as, backup and restore, business continuity and phishing training. Risk should be measured by your capabilities in these controls.

In cybersecurity, risk and cost are typically linked. Investment is required to improve controls, and lack of investment results in less effective controls that equates to more risk. Unfortunately, it is also true that the mere act of making an investment does not necessarily improve controls and reduce risk. Therefore, Gartner recommends measuring control effectiveness through outcome-driven metrics which measure the outcomes of a control, not just the existence of the control or it's maturity. Outcomes are a better measure of the benefits and actual protection levels provided by a control (see “Outcome-Driven Metrics for Cybersecurity in the Digital Era”).

**The Cost Dimension**

The cost dimension measures the costs related to managing and treating risk such as tools, development, insurance and business process changes. Figure 1 presents cost as the size of the stars representing the targets.

- **How much are you willing to invest to address risk?** Risk levels can be treated and managed through explicit investments (cost) designed to address known risks.

- **How well will cybersecurity be funded?** The organization can choose to fund cybersecurity generously (lower risk) or fund it minimally (increased risk).

- **What are the priorities and investments to achieve your desired level of protections?** Risk levels can be treated and changed through dedicated investments specifically designed to address cybersecurity risks.

Cost is not just budget and money; it is anything that creates a cost to the organization related to the identified risks, such as impacting customer experience. For example, multifactor authentication in a mobile online banking application manages the risk of unauthorized transactions at the expense of the customer experience. This is considered an investment (and cost) to lower risk. Both inherent costs and chosen investments are included in the cost dimension.
It is a business decision to choose any level of investment. Together the risk and investment dimensions represent possible risk decisions from saving investment and experiencing more risk on the left to making investments and experiencing less risk on the right.

The Risk Optimization Zone

RVC optimization is ultimately a business decision, in a business context, that is credible and defensible to the identified stakeholders. The risk optimization zone in Figure 1 is a simple representation that assumes it is credible and defensible for lower value targets to have more risk and lower investment. And that higher value targets should have higher investment and commensurately lower risk. Targets that fall out of the risk optimization zone should be subject to further assessment and treatment.

In practice, an organization can choose to draw or define the risk optimization zone in any manner that supports credible and defensible business decisions related to cybersecurity readiness. And any given target may be credible and defensible outside the risk optimization zone, but it should have a business case with recommendations defending its position as credible and defensible. Risk appetite may reshape how an organization determines that a risk has been optimized.

Also in Figure 1, the dimensions of risk (x-axis) and value (y axis) create a two-by-two matrix with four quadrants. The characteristics of these quadrants provide a guide for interpreting and addressing the positions of various targets (see Note 1 for more explanation of the quadrants).

Smaller, less complex organizations can optimize risk by accepting more risk with lower investment and still meet the expectations and needs of their key stakeholders. Higher levels of investment may result in levels of protection that exceed the needs of the organization to remain defensible with stakeholders.

Larger, more complex organizations generally need to spend more and have higher levels of cybersecurity capability to meet the needs of their stakeholders like regulators and investors. They can plot the cybersecurity readiness of business functions to see the relative levels of risk in the context of business criticality to drive priorities and investments.

Large conglomerates can also plot the cybersecurity readiness of business units to understand where risk has not been optimized to drive priorities and investments in cybersecurity. In this case, value could be plotted as revenue.
Stakeholder Credibility and Defensibility

Organizationally, key stakeholders are commonly those above the decision maker, such as the executive committee and board. But more importantly, key stakeholders are constituencies that are served by the organizational outcomes such as customers and shareholders or, in government agencies, the citizens. They can also be bodies with oversight power like external auditors or regulators.

Each of these constituencies have expectations and needs that should be served appropriately by decisions, priorities and investments. Proactive and formal consideration of these expectations and needs will influence the decisions, priorities and investments to create better outcomes for all.

Will your board, shareholders, customers and regulators agree that your chosen investments, priorities and risk acceptance meet their expectations and needs?

The following are some examples of cybersecurity decisions that lack credibility and defensibility through the lens of stakeholder needs:

- A choice to continually accept technology debt to keep IT costs lower. The CFO may cheer the lower costs, but with full visibility into the risk of eventually facing a major investment to upgrade a failing infrastructure would not pass the RVC optimization test.

- A choice to purchase a point of sale system that will fail to meet regulatory requirements in six months due to rule changes. A business decision maker can expedite a purchase to meet immediate needs within budget constraints, but this would not be credible or defensible for regulators or executives.

- A choice to give product managers freedom to use customer analytics without sufficient rigor to control unethical use of the data. Product managers may even be encouraged to exploit analytics and push boundaries, but this would not pass the RVC optimization test with customers and many shareholders, including the European regulators managing the General Data Protection Rule (GDPR).

- A choice to work with a third-party provider that fails cybersecurity readiness assessments. This may or may not be risk optimized based on the criticality of the supplier, the level of risk and the business outcomes it supports.
Business Context

CIOs and chief information security officers (CISOs) have understood for years that technology investments should always be made in a business context that supports the achievement of business outcomes. And yet they struggle to execute.

It is critical to bridge the gap between technology and business decision making. This is done by selecting targets, assessing value and assessing risk, all in a business context. Targets should be business units, business process or other constructs that are directly connected to the achievement of business outcomes. Value should be assessed in terms of business outcomes like revenue, margin, productivity or other value directly connected to a business context. And risks should be directly related to and viewed in the context of impact to business outcomes.

For RVC optimization, we define a business context as a direct causal relationship to a business function, process, outcome or other business orientation that would be in the sphere of responsibility for a non-IT executive. For example, in a financial services institution, non-IT executives care about the mortgage lending, core banking, branch operations, trading and the ATM network. Isolating the infrastructure and the parts of the application portfolio that support those functions puts those technology elements in a business context.

If we extend this example, we can describe levels of protection for each of these because controls and effectiveness vary across these business functions. Perimeter protection is greater for core banking because it is behind multiple layers of controls, while branch operations have less perimeter protection because the branches are closer to the customer and require more direct access to the internet. Similarly, threat and vulnerability management varies because mortgage lending services are patched faster, while online banking services are patched slower because they have 24/7 business availability needs.

Using this definition, the need to spend $1 million on security information and event management (SIEM) to “protect the business” is not viewed in a business context. No executive knows or cares what a SIEM is, and protecting the business is a platitude that they already consider the CIO’s responsibility.

An opportunity to invest $1 million to improve detection of unauthorized activity in online banking operations to reduce unscheduled outages is viewed in a business context. The presentation of this as an opportunity to invest engages the executives to consider this investment versus others to protect their business outcomes in a business context.
The key to using business context successfully is using it to focus and engage the executives without getting bogged down in the details of covering every aspect of security. There are many moving parts of cybersecurity that do not require their engagement. When you speak to non-IT executives you should only share that which is meaningful to them in a business context.

**Determining Cost**

Cost should be determined as the collective costs to address the known risks specified in the risk assessment. In the ransomware example above, cost would be the people, process and technology costs needed to deliver readiness across the three primary ransomware controls of backups, business continuity and phishing training. Each business unit would have different costs and differing levels of readiness based on their execution of those three controls.

**Assessing Value**

Value is also dependent on the context of the decisions that need to be made. It can be size, scope, revenue, margin, criticality or any combination of elements that define relative value for the targets being assessed. Value should be expressed in a manner which is understood by the decision makers and in the context of the decisions that are being made. If you do not understand the relative value of the targets you are assessing, then you should discuss this with your executives and describe value the way they describe value.

**Using the Model**

The model is designed to provide a comparative analysis of business outcomes in the context of their value, the risk they are experiencing and the costs related to addressing their cybersecurity risks. To use the model, assess risk, value and cost of various targets to drive prioritization and investment decisions. A variety of targets can be plotted on the RVC optimization model to support decision making, including initiatives, identified risks, projects and business units.

This information and representation supports credible and defensible business decisions to optimize risk. It is through the lens of stakeholder credibility and defensibility that determines when cybersecurity risk and investment have been optimized.

**Step by Step**

This model can be used to create credible and defensible RVC optimization for any program, project or initiative by following these steps:
Assessing Cybersecurity Risk

Organizations can get distracted by a need to have “perfect” cybersecurity risk assessment when they only need enough rigor in their assessments to support credible and defensible decision making. There are times when rigorous, quantitative risk assessment is possible and warranted. There are other times when qualitative, consensus building (regarding levels of risk) is sufficient to support credible and defensible decisions.

- Define the target or targets to be optimized for cybersecurity risk (e.g., business units).
- Assess each target’s risk based on readiness to address cybersecurity risks (e.g., in ransomware, readiness to deliver backup, business continuity and phishing training by business unit).
- Determine the cost to deliver the level of cybersecurity readiness for each business unit (e.g., cost to deliver the readiness of the three primary ransomware controls in each of the business units).
- Assess the value of each target in a context that will be meaningful to the decision makers.

Plot the targets in a visual model, as described above, and develop a narrative to accompany any business case, oversight report or funding request related to cybersecurity:

- Describe the stakeholders and their needs.
- Identify targets that are not optimized for risk. Essentially, those that are so far outside of credibility and defensibility that they address stakeholder needs for investment and risk.
- Develop a prioritized plan of investments to optimize cybersecurity risk for these targets.
- Describe how the recommended priorities and investment will balance the needs to manage risk with the needs to achieve the desired business outcomes, and how these proposed investment address stakeholder needs and optimize risk.
As described above, Gartner recommends risk posture for cybersecurity should be measured as a function of control readiness to address identified threats, not the risk of the threats themselves. It is up to each organization to determine how best to assess risk depending on the decisions that need to be made. Here are four options for measuring cybersecurity capabilities to optimize cybersecurity risk in this model. Most organizations will use a combination of all of these:

**Benchmark Cybersecurity Spending (Strongly Not Recommended).** Benchmark spending on security is a poor barometer for determining capabilities. Organizations exist that have high spending and poor levels of readiness/capability as well as organizations that have low spending and high levels of readiness/capability. Intersecting spending with maturity only tells an organization their price for performance. The amount spent on security should be commensurate with a plan to build an appropriate level of capability/readiness that matches business need.

**A Maturity Model (Recommended, but Limited).** Maturity models have been common since the early 2000s as a representation of security capabilities and remain the state of the art in 2020. There are many choices in the marketplace, including industry-specific options and those that have global benchmarks. The primary limitation of maturity models is that after an organization achieves a maturity level of 3 or higher, the maturity model itself is less useful for determining priorities and investments to improve. And maturity models are blunt instruments typically based on relatively few questions.

**Third-Party Assessment (Recommended, but Costly).** Paying a third party with subject matter expertise to assess and formally benchmark your organization is a very effective way to understand gaps and opportunities for improvements in controls. Depending on the size of the organization these can cost $75,000 to $500,000. Some Gartner clients have observed that they get cut and paste results and there is almost always a recommendation for follow-up work from the assessor to address the identified gaps. This can be considered a conflict of interest impacting the trustworthiness of the results. However, the value of a third party, the detailed benchmarks and the customized results make this worthwhile at least once every three years.

**Outcome-Driven Services and Metrics (Forward Looking, but Very Promising).** Outcome-driven services and metrics are a more accurate reflection of the delivered levels of protection for business functions and outcomes. For example, an outcome-driven threat and vulnerability management service would patch systems within a chosen number of days supporting a particular part of the business. And outcome-driven metrics would report the operational delivery of the actual number of days in which the systems were patched (see "Outcome-Driven Metrics for Cybersecurity in the Digital Era").
The business chose to patch systems supporting core banking within 20 days and operationally they succeeded in patching 80% within 15 days, 15% within 22 days, and 5% are currently at 30+ days because of business decisions to miss scheduled outage supporting 24/7 business operations.

This powerful new approach creates a direct reflection of the protection provided and supports business decision making related to levels of protection in a business context. It will require material investment and significant advancement to achieve this level of capability, but given the limitations of current approaches, we believe this is inevitable to address regulatory demands and shareholder expectations (see “An Outcome-Driven Approach to Cybersecurity Improves Executive Decision Making”).

**Identifying Stakeholders in Cybersecurity**

The stakeholder lens in RVC optimization surfaces in the business cases to support conscious business decisions. Stakeholders should be identified and their needs summarized at the beginning of an optimization process to demonstrate the consideration of stakeholder needs. Identify elements of the assessment that are not credible or defensible for key stakeholders then create a conclusion that summarizes material decisions that impact and address stakeholder needs (see Note 2 for a list of common stakeholders in cybersecurity).

**Factors Influencing Credibility and Defensibility**

Several factors may play a role in determining that business decisions are credible and defensible to stakeholders:

**Transparency of decisions.** Transparency is a major factor in credibility and defensibility. If relevant information is kept from stakeholders and/or decision makers then credibility and defensibility is hard to achieve. Common examples include avoiding recognition of gaps and opportunities for improvement, and failing to acknowledge that some risks are inevitable but are appropriate to achieve desired results.

**Appropriately engaged executives.** If executive decision makers are not engaged in the decision-making process this leads to indefensible positions that lack credibility.

**Avoiding inconsiderate engagements of risk.** This occurs when an executive makes an expedient decision without full knowledge of the impact. For example, broken accountability where an executive will sign off a decision to meet their business needs, without full consideration of the impact on the organizations larger business needs.
Effective risk-based governance. This is when a risk process enables the negotiation of appropriate controls to achieve business outcomes.

Appropriately rigorous risk assessment methodology. There should be enough investment in the assessment process to get good information.

See Note 3 for a decision tree to optimize risk through the lens of credibility and defensibility.

See “A Decision Model to Optimize Risk, Value and Cost” for more examples and context to implement RVC optimization in cybersecurity.

Case Study
A small chemical company (700 people) was sold to a large conglomerate after years of neglecting investment in good cybersecurity. The CIO and CTO were concerned about going in front of the new board to explain their current state of cybersecurity readiness and capability. Cybersecurity had clearly been a board issue for years, but their previous board had suffered from the cultural disconnect and relied on the technical people to just handle the issue without any material uplift investment in capability.

Using the RVC optimization narrative with their board would bridge the cultural disconnect and allow them to position their current state of readiness as a reflection of legitimate business decision making by previous management. The company had no direct retail consumer packaged goods brands, no sensitive PII and no history of material breaches. They had acceptable foundation security controls such as patching, endpoint security and backups, but it was clear that there were gaps and opportunities for improvement in capability.

The RVC optimization model presented their new executive management and board the opportunity to make different decisions. They too faced the legitimate business decision to push on the accelerator and invest in better security capability or remain with the modest controls they had in place. Changing the conversation to a business decision over a level of investment for a level of protection put stakeholder defensibility at the center of their choice and created defensibility for the CIO and CTO.
Note 1
Treatment Quadrants in a Risk, Value and Cost Optimization Model

In Figure 1, the dimensions of risk (x-axis) and value (y-axis) create a two-by-two matrix with four quadrants. The characteristics of these quadrants provide a guide for interpreting and addressing the positions of various targets (see Table 1).

Invest (Upper Left)
The invest quadrant is defined by high-value, high-risk targets that are likely underinvested. These targets require business cases that describe their circumstances and recommended treatment options. Essentially, these will likely require some investment to bring them in line with a risk-optimized position that is credible and defensible to stakeholders.

Cut (Lower Right)
The idea of cutting cybersecurity is anathema to traditional cybersecurity professionals, but it is a powerful message to executives that cybersecurity is always a choice and not every part of the organization needs to be protected at the same level. The cut quadrant is characterized by targets that are lower value, lower risk and potentially overinvested. These targets require business cases that defend their level of investment for the value they deliver.

Opportunity (Lower Left)
The opportunity quadrant is characterized by targets that are lower value, lower risk, and lower investment. These are opportunities to be explored for further investment, and the RVC optimization model can be used to increase value and commensurately manage risk.

Manage (Upper Right)
The manage quadrant is characterized by targets that are higher value, higher investment and commensurately manage risk to appropriate levels. These targets should be managed and monitored to ensure that investments and risk remain at credible and defensible levels.
### Table 1: RVC Optimization Treatment Quadrants

<table>
<thead>
<tr>
<th>Quadrant</th>
<th>Value</th>
<th>Risk</th>
<th>Investment</th>
<th>Treatment (Build a Business Case)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invest</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>Recommendation to address risk that is credible and defensible</td>
</tr>
<tr>
<td>Cut</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>Defend or cut investment</td>
</tr>
<tr>
<td>Opportunity</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>Opportunities to increase investments for higher value</td>
</tr>
<tr>
<td>Manage</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Manage and monitor to maintain appropriate risk and investment</td>
</tr>
</tbody>
</table>

Source: Gartner (February 2020)

**Note 2**

**Cybersecurity Stakeholders**

Cybersecurity has many stakeholders. It's important to identify them with their context, needs and expectations related to risk and security. Here is a partial list of common stakeholders for cybersecurity:

- **Customers.** Typically these will be end-user customers who buy/use the products and services of the organization. Their context will vary across the amount of sensitive data they share, their relationship to the organization, their privacy concerns and so on. This consideration is critical when faced with decisions related to protection versus customer experience.
Regulators and oversight bodies. Regulators themselves have shifted over the last 10 years away from checkboxes to requiring a consideration of business outcomes and need when selecting controls. They are looking for transparency and defensible decision making.

Boards of directors. Boards have a fiduciary obligation to provide oversight for risk and security. Most board members do not understand that security is a choice. Once this misunderstanding is reset and they view this as a business problem (investment for a level of protection), boards can become important allies in determining appropriate balance.

Shareholders. Shareholders are the mirror image of customers. They want business outcomes and view risk as opportunity. Balancing shareholder needs with customer needs is where some of the toughest decisions must be made. For example, the use of analytics to monetize customer data.

Elected officials. In government agencies, elected officials and career bureaucrats tend to view security as a compliance exercise. Helping them to understand the risk-based approaches that support initiatives like e-government and digital transformation will also help guide the right balance for cybersecurity.

Other stakeholders. Every industry and every organization will have unique stakeholders and unique needs. Identify them, understand them, understand the organizational politics and use their unique expectations and needs to guide your decisions. Examples include family-run businesses, startups, holding companies and foreign-owned subsidiaries.

Note 3
A Decision Tree To Optimize Risk and Value

Once you have plotted your targets and described their positioning to the decision makers, use this decision tree to address and optimize known risks:

- Has sufficient rigor and investment been made in assessing the risk and value of these targets?
- Do we have the right executive decision makers in the process?
- Is there enough transparency to make fully informed decisions?
- Do we sufficiently understand the needs of the relevant stakeholders such as our shareholders, regulators and customers?
For each target:

- Does the risk and relative value of the target create a credible and defensible case that balances the needs of relevant stakeholders?

For each target that is not credibly and defensibly optimized for risk:

- What are the circumstances for the targets positioning?
- What are the needs and considerations of the relevant stakeholders?

---

**Recommended by the Author**

Some documents may not be available as part of your current Gartner subscription.

IT Cost Optimization, Finance, Risk and Value Primer for 2020

A Decision Model to Optimize Risk, Value and Cost

The CARE Standard for Cybersecurity

Outcome-Driven Metrics for Cybersecurity in the Digital Era

An Outcome-Driven Approach to Cybersecurity Improves Executive Decision Making

The Urgency to Treat Cybersecurity as a Business Decision
Position your IT organization for success. Explore these additional complimentary resources and tools for security and risk leaders:

**eBook**
3 Steps to Stop Employees Taking Cyber Bait
Bring cybersecurity awareness to your organization today to change employee behavior and manage risks effectively.

**Roadmap**
Protect Your Business Assets With a Roadmap for Maturing Information Security Program
Build a mature information security program to mitigate cybersecurity risk effectively.

**Research**
How to Prepare for Ransomware Attacks
Prepare for the security challenge organizations are facing today.

**Webinar**
3 Ways to Gain Support for Your Security Awareness Program
Effectively communicate the value of your security awareness program.

Already a client?
Get access to even more resources in your client portal. Log In
Get More.

Get actionable, objective insight to deliver on your most critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance. Contact us to become a client:

**U.S.:** 1 855 811 7593

**International:** +44 (0) 3330 607 044

Become a Client

Learn more about Gartner for IT Leaders
gartner.com/en/information-technology

Stay connected to the latest insights