5 Steps to Cost Optimization for Security and Risk Leaders in Uncertain Times

Organizations are ill-prepared to confront the impact of crises on their services and goals. As economic and work environment uncertainty increases, security and risk management leaders must create a cost optimization plan to aid their organizations in navigating past this challenging turn.

Additional Perspectives

Summary Translation: 5 Steps to Cost Optimization for Security and Risk Leaders in Uncertain Times
(22 June 2020)
Overview

Key Challenges

- The current economic and health crisis will have a negative impact on security budgets across many industries. This is especially concerning given the increased dependence upon digital systems that organizations have undertaken in response to COVID-19.

- Organizations tend to focus and prioritize most of their resources toward responding to a crisis. This impedes their growth during the recovery phase where focus must be on operational stability.

- Cost optimization efforts are not balanced and primarily focus on “cost reduction” rather than optimization, which may include exploring alternative delivery platforms, outsourcing, increased spend, employee retention and other mechanisms.

- Security and risk management leaders and their programs are ill-equipped to deal with budgetary challenges, in part due to a static and informal planning and budgeting process.

- Organizations could suffer business consequences if they wait out the impact of a crisis such as COVID-19: Time is of the essence.

Recommendations

Security and risk management (SRM) leaders must facilitate business outcomes through an effective cost optimization strategy as follows:

- Identify the crisis phase (triage, doldrums, recovery) that the organization is working around and equip your team with relevant data (such as benchmarking) to support these efforts before jumping into the exercise.

- Build adaptable “budget scenarios” that reflect the reality of your security and risk management function should you find yourself in a situation that requires immediate and decisive action (for example, large budget cuts).

- Align security and risk services with the value of a business unit to optimize cost and risk. This helps identify critical points to shield and noncritical items to eliminate/reduce.

- Balance efforts to ensure that you are not solely focused on “reduction in spend,” but rather on a budget portfolio that drives efficiency, productivity and optimization.
Align your efforts with roles, competencies and skills that currently exist in the organization to ensure efficiency.

Strategic Planning Assumption

By 2023, 30% of a CISO’s effectiveness will be directly measured on the ability to create value for the business.

Introduction

With the COVID-19 crisis reaching the peak of impact in many countries around the world, organizations are scrambling to control and manage disruptions to their business. A recent poll of Gartner’s client community found that nearly half of respondents are experiencing reduced effectiveness, and in some cases severely so, as a result of COVID-19 (see Figure 1).

Figure 1. Impact of COVID-19 on Standard Business Outcomes

<table>
<thead>
<tr>
<th>Impact of COVID-19 on Standard Business Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>50%</td>
</tr>
<tr>
<td>25%</td>
</tr>
<tr>
<td>0%</td>
</tr>
<tr>
<td>Business operations continue as normal</td>
</tr>
<tr>
<td>There is little disruption to business operations</td>
</tr>
<tr>
<td>Business operations continue at a reduced level</td>
</tr>
<tr>
<td>Business operations are severely restricted</td>
</tr>
<tr>
<td>Business operations cannot continue</td>
</tr>
</tbody>
</table>

n = 833 Gartner Research Circle Members

Q: How has the Novel Coronavirus (COVID-19) affected standard business operations in your organization?
Source: Gartner COVID-19 Research Circle Poll, 16-17 March 2020
ID: 722885_G
This economic uncertainty is almost certainly going to drive cost pressures and budgetary reallocations in the near term. This is especially critical for security and risk functions that operate within the context of an IT budget. Gartner has indications that leaders are not prepared for the extent of the budget pressure or severity of impacts. Indications such as the increasing threat landscape, digitalization, and an increasing third-party ecosystem, leaders are also challenged to adapt their budgets (see below).

82% of security and risk leaders do not adapt their budget to business or environmental impact.

— IT Score for Security and Risk Management

In addition, a large majority of security and risk leaders reported that their budgets had either flattened or lowered in the past 12 months, just prior to COVID-19. This is mainly due to the lack of triggers as part of a formalized planning and budgeting process (see Figure 2).

Figure 2. IT Security Spending as a Percentage of Total IT Spend

<table>
<thead>
<tr>
<th>Year</th>
<th>YoY Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>5.6%</td>
</tr>
<tr>
<td>2016</td>
<td>5.9%</td>
</tr>
<tr>
<td>2017</td>
<td>6.2%</td>
</tr>
<tr>
<td>2018</td>
<td>6.0%</td>
</tr>
<tr>
<td>2019</td>
<td>5.7%</td>
</tr>
</tbody>
</table>

Source: Gartner (2019)
* Range includes the 5th to 95th percentile of the sample.
ID: 485697
Gartner expects that COVID-19 will be a catalyst for security budgets to shift significantly. To support this, a survey of Gartner's senior finance leaders suggested that IT organizations are expected to face 10% or higher budget cuts in 2020 as a result of COVID-19 (see Figure 3).

**Figure 3. SG&A Functional Cuts**

The near to medium term will be all about business continuity and facilitating business outcomes through an effective cost optimization strategy.
This strategy must aim to drive spending and cost reduction while maximizing business value. Moving forward, security and risk management leaders can no longer afford to “wait.” Leaders will be forced to make decisions on focus areas and concessions to drive additional cost optimization efforts. To support the initial effort, Gartner has published tactical research to support SRM leaders in the near term (see "Be Resilient: Prepare to Treat Cyber Risk Following the Coronavirus [COVID-19] Outbreak by Focusing on These 7 Areas"). The following analysis aims to equip leaders with techniques that they can use to navigate out of this challenging turn in the next 12 months.

**Analysis**

**Identify the Crisis Phase That Your Organization Is Working Around**

Before using any of the techniques detailed in this research, leaders must first strategize for the crisis phase that the organization is currently navigating. In “Manage an Economic Downturn in 3 Phases,” Gartner introduces the three phases to a crisis (see Figure 4). Security and risk management leaders must identify the crisis phase that their organization is currently going through in order to drive the most effective cost optimization efforts.

**Figure 4. Managing the Three Phases of a Crisis**

---

**Managing the Three Phases of a Crisis**

- **Phase 1: Triage**
  - Where we are right now
  - Surprise, volatility
  - Need for prompt action
  - 20% or more budget cuts common
  - Lower operating costs

- **Phase 2: Doldrums**
  - Number of new cases levels off
  - Deceptively quiet
  - Uncertainty of both downturn, recovery
  - Sustaining what exists
  - Starting investments in growth initiatives

- **Phase 3: Recovery**
  - Extraordinary measures ended
  - Rising optimism
  - Urgency for investments
  - Budgets remaining tight
  - Investing 5% to 10% in innovations

Source: Gartner 722658_C
This initial step allows SRM leaders to frame their decisions using a formalized structure. Leaders can structure efforts across the different phases and communicate those efforts in a visual manner. They can also prepare for potential budget cuts/requests by understanding what level of crisis the organization is trying to navigate out of. Lastly, this adds to the personal leadership qualities that are very visible during different phases of a crisis — i.e., it elevates your function from being a cost center to one that provides value to the business by aligning with the phases.

SRM leaders should begin by triaging, which usually has very volatile and uncertain outcomes. It results in lowered revenue and earnings expectations, headcount reductions, asset sales and restructuring. In this phase, businesses move to conserve cash, and those that have accumulated reserves view the crisis as an economic opportunity to grow. It is also not uncommon to hear of budget reductions up to 20% and lower operating costs. This is time for immediate and decisive actions that are unplanned. The majority of organizations are currently in this phase when it comes to COVID-19. In this phase, SRM leadership must be ready to make hard, and potentially unpalatable, emergency cost-cutting decisions. Identify and discuss potential emergency cost-cutting opportunities as soon as possible.

In Phase 2, the crisis will have reached its peak; this is when economic decline tends to set in. This usually results in delays in future investments until the situation is fully resolved. Here, leaders will be forced to sustain what currently exists, with some preliminary planning taking place. SRM leaders must now take a more strategic look at cost optimization (not just cost cutting) opportunities.

In Phase 3 recovery starts. The flow of credit/cash continues to show improvement, and investment becomes critical to sustain growth. The final phase is what differentiates top growth organizations from others. In this phase SRM leaders must identify where selective, focused investment can help the business accelerate. This must be done in conjunction with the business and IT strategy for recovery. The average organization will have committed most of its resources to Phase 1 and Phase 2, resulting in a slow pace of recovery and growth; whereas an effective cost optimization strategy will have positive results on the SRM function.
Equip Your Function With Relevant Data to Support Cost Optimization Efforts

With the way that the current crisis is unfolding, every research organization is scrambling to produce forecasts, information, models and historical context to predict the future of the global economy (see “Forecast Analysis: Global Recession Scenario”). This goldmine of information must be incorporated into the cost optimization effort, especially as different stakeholders begin to get involved in the process. Gartner suggests that SRM leaders focus on four layers of data:

1. **Benchmarking** — Many organizations, including Gartner, publish annual benchmarks associated with the security and risk management function. Gartner's IT Key Metrics Data (see "IT Key Metrics Data 2020: IT Security Measures —Analysis") benchmarks organizations using a variety of spend factors across multiple industries. For security functions that are navigating a crisis for the first time with no baseline, benchmarks can be a good starting point. Gartner cautions leaders not to use benchmarks as sole data points to justify business decisions, but rather as more of an additional data point or reference/evidence.

2. **Current-state assessment** — SRM leaders can also get an overview of their capability maturity by completing the "IT Score for Security and Risk Management." This aids leaders in identifying areas of importance as well as gaps in the overall security program. Keep in mind, maturity models tend to have limited impact on risk, value and cost as they rely on your ability to make the right decisions using the right combination of information, knowledge and skills. Leaders are also encouraged to monitor activities around the organization and use them as lessons learned for future cost optimization efforts. Leaders cannot afford to make any changes during the first phase of a crisis, but they can build defensible business cases for future recovery efforts.

3. **Threat landscape** — Threat landscape reports exist in a variety of formats published by leading security vendors and technology service providers. This information allows leaders to incorporate and compare common threat vectors that emerge before, during and after a crisis. Typically, vectors such as phishing, social engineering, credential thefts, and nation-state attacks operate at a different pace in volatile periods. In addition, leaders can use frameworks like the MITRE ATT&CK framework to model their threat landscape and ensure that they reallocate spend to critical services. Gartner cautions leaders not to inflate the applicability of the threat landscape. Leaders have no control over the pace or types of threats; and, as such, longer-term planning in this area is not recommended.
4. **Business-related data** — Arguably, this is the most important layer of information as it correlates directly with your ability to facilitate business outcomes. Have your organizational goals changed as a result of the crisis? Is there competitive analysis data that you can refer to? Listen to and incorporate quarterly earning findings into your strategy. This layer of data is within your control and points to business expectations of security. Organizations that are good at modeling their operational risks will have an advantage over their less-skilled competitors in this phase, as they are likely to make more effective decisions. Once leaders nail this down, they can identify additional cost optimization opportunities and achieve competitive advantage.

**Build Adaptable “Budget Scenarios” That Reflect the Reality of Your SRM Function**

Leaders have to be able to balance fast reaction times in response to this crisis with careful planning and budgeting processes that require a much slower pace. To assist with this, SRM leaders should look to build adaptable budget scenarios that address operational decisions in times of need. Chief financial officers and other executives run this exercise on a regular basis, therefore, SRM leaders are encouraged to align with the efforts that their finance team is undertaking as part of the overall cost optimization process. The budget scenarios should clearly lay out strategic steps that you will take to respond to that specific scenario, understanding that these steps will be dependent on your business environment. For each one of the scenarios outlined below, you may also want to create a base-case, worst-case and best-case approach.

**Emergency budget cut:**

- **Worst Case:** For example, function A was asked to cut spending by half by the end of Q2.

This scenario can be activated when there is an immediate action to deal with severe business interruption. This is usually associated with drastic budget cuts to ensure immediate business survival. Focus on foundational and essential investments that allow you to function in survival mode. What are the barebone essentials that you will need? There will be risk — think about how you will manage this.

**Selective cost reductions:**

- **Base Case:** For example, security function B was asked to cut spending by 10% every quarter for the next year.
This scenario is activated when there is a longer-term impact to business goals. This is usually associated with consistent budget cuts across all departments through a longer time frame to ensure cost optimization. Here, efforts should be targeted at the investments that will deliver the least harm to business goals.

Preserving costs and business growth:

- **Best Case:** For example, security function C has been asked to maintain the budget, but focus heavily and clearly on delivering business value.

This scenario is activated when, despite any impact or interruption, the business decides to maintain current levels of spend based on future outlook. Here, best practices should be maintained. Costs should be preserved where investments have been defined as critical to the high value business units.

### Table 1: Sample Budget Scenario — Emergency Budget Cut

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Situation Description</th>
<th>Impact to Function</th>
<th>Impact to Business/Stakeholders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency budget cut due to COVID-19</td>
<td>Severe business disruption due to COVID-19 forcing a 50% reduction in spend by Q2.</td>
<td>Enable workforce through securing remote working capabilities. Consider layoffs.</td>
<td>IP and/or PI leak due to increased remote working capabilities with limited monitoring. Customer service portal to suffer from bandwidth issues. Project delays.</td>
</tr>
</tbody>
</table>

Source: Gartner (April 2020)

**Align Security and Risk Services With the Value of a Business Unit to Optimize Cost and Risk**

Optimizing cybersecurity risk in a business context through the lens of the business unit creates a powerful model to drive decisions related to prioritization and investments. This also 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 need to address risk and the need to achieve its desired business outcomes.
This is where your real cost optimization strategy begins. The level of cybersecurity risk experienced by each business unit is plotted against business value. SRM leaders can now optimize risk in a business context through the lens of stakeholder credibility and defensibility (see Figure 5).

**Figure 5. Optimizing Risk, Value and Cost for Security Readiness**

In the example in Figure 5:

- **Business Unit A** is very business-critical (contributes 30% of top-line revenue, in a regulated industry, has a lot of personal information [PI]) 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. Leaders need to invest in services that fall within this area to ensure appropriate risk is commensurate with cost and value.

- **Business Unit B** has lower business criticality and commensurately less need for high cybersecurity capabilities (no PI, less sensitivity to unscheduled outage), so it may be credible and defensible to have higher cybersecurity risks and lower investments in addressing it. Leaders should create a business case to limit services to these business units in times of economic uncertainty.
Business Unit E has high business criticality with commensurate levels of investment to create good cybersecurity capabilities within acceptable levels for shareholders and regulators. Leaders should maintain services that fall within this area to manage appropriate risk and investment costs.

Business Unit F has low business criticality, but higher levels of investment to create world-class cybersecurity capabilities. It may be appropriate to suggest to the CFO that Business Unit F has overinvested in the latest technology advances to maintain an unnecessary level of cybersecurity protection. Leaders should take advantage of opportunities that fall in this area to cut baseline costs.

For further insight into Gartner’s risk, value and cost optimization model, see “Optimize Risk, Value and Cost in Cybersecurity and Technology Risk.”

**Balance Cost Optimization Efforts to Ensure You Are Not Solely Focused on “Spend Reduction”**

It may be difficult to envision during a disruption, but cost optimization does not always mean “reduction in cost.” An effective cost optimization strategy aims to balance efforts across major portfolios of services. For example, to address certain new realities like remote working, leaders will almost certainly not reduce any spend in this area. Instead, they will extend VPN to all employees after evaluation of technical debt and cost (see “Quick Answer: Cost Effectively Scaling Secure Access Now and Preparing for a Remote Workforce”). In certain cases, a more strategic change may bring results that will provide savings in the longer term. Gartner has identified “The Four Levels of Cost Optimization” as a planning and communication structure to deliver a balance of strategic and tactical cost control. Security and risk management leaders can use the model in Figure 6 to justify decisions in certain areas against a backdrop of business outcomes.
Figure 6. Take a Portfolio View of Cost Optimization

The four paths that can be taken, individually or together are:

- **Contract Management**: In times of economic uncertainty, sacrifices and concessions will have to be made. For example, you may need to get creative and use a combination of open-source and paid services. You may decide to forgo your on-premises security operations center for a hybrid model that prioritizes a SaaS model. You can also use Gartner’s BuySmart service to negotiate better prices and discounts for your current contracts.

- **Cost Savings Within Security/IT**: Most cost optimization efforts today tend to revolve around cost savings associated with an internal function such as security, especially in times of crisis. Simply put, leaders need to identify opportunities to reduce or eliminate baseline costs. For example, you may decide to automate/triaging manual tasks such as log management, or to outsource operational capabilities, such as monitoring to a managed security service provider (MSSP). You may also decide to take on your organizational structure and delegate security functions such as architecture, system engineering and development to relevant teams in IT-business. You may decide to postpone or cancel all nonessential projects, or, worse, reduce your talent requirements by combining one or more roles. For additional analysis on how to “reduce” spending during mandatory budget cuts, see “How to Respond to Mandatory IT Budget Cuts.”
Joint Business and Security Cost Savings: Considering that the average security function spends $2.84 for every $1,000 that the business generates in revenue,¹ cost optimization efforts here should provide a dual impact on both the function and the business. This can be done through modernization, different delivery platforms and alternative acquisition models. For example, you may decide to make concessions in your password access protocols and implement a self-service reset tool. You may look at areas where security spend is not aligned with risk and thus identify opportunities to reduce spend. You may institute a process where the business units are trusted with doing their own risk assessments. Efforts in this area help leaders evolve from cost cutting to value optimization (see “Smarter Spending: Invest in Business Outcomes”).

Business Optimization: Gartner predicts that by 2023, 30% of a CISOs’ effectiveness will be directly measured on their ability to create value for the business. This area is where value generation tends to happen (see “Predicts 2020: Security and Risk Management Programs”). For example, you may decide to adopt a new identity provisioning system to be executed by business owners and HR. You may decide to provide services to the business using defined SLAs that can be charged back to individual high-value business units. Leaders should supplement this area with services that reposition security as a competitive advantage and a value generator for the business.

Aligning cost optimization efforts with the four levels of cost optimization can help leaders determine if their overall cost optimization effort is out of balance (for example, all cuts coming from cost savings in IT/security). Conversely, it can determine whether the organization has mixed cost savings with other optimization techniques, such as business restructuring and innovation to prepare the organization for a return to growth.

Remember, all of these cost optimization initiatives will have opportunity cost and risk associated with them — they all represent some trade-offs. Finally, leaders can also choose to assess each potential cost optimization initiative against the criteria outlined in “Gartner’s Decision Framework for Prioritizing Cost Optimization Initiatives” to help prioritize them based on their potential respective impact and risk (see Figure 7).
Align Efforts With Roles, Competencies and Skills That Currently Exist in the Organization

Uncertainties such as COVID-19 have an unprecedented impact on the way you recruit, develop and retain talent. Many industries, such as travel, hospitality and retail, have completely shut down their workforce, while other industries, such as healthcare, are shoring up essential personnel and reducing their nonessential workforce. In response to this, SRM leaders may find themselves at a crossroad. Inevitably, cost optimization will also be extended to human resources.

However, as previously indicated, your efforts have to be balanced and not focused on one area of optimization, such as workforce cuts. The end goal should be related to enabling the business. This may require layoffs, additional hires, reallocation of skills and talent sharing, among other techniques.

In an effort to support leaders, Gartner recommends that you align all of your cost optimization efforts back to your personnel needs using a combination of roles, skills, and competencies.
SRM leaders should:

1. Differentiate between roles, skills and competencies (see “Focus on Competencies to Establish Security and Risk Expertise in a Digital World”). This is especially critical as you begin to identify the minimum combination of roles, skills and competencies required to help the business operate in times of uncertainty. Remember that addressing new skills or competencies does not mean you need to hire new talent. Look for opportunities to share talent between functions and identify cross-functional training opportunities, such as apprenticeships, to leverage individuals. This allows you to build broader talent pools, transferable skills and offer flexibility during uncertainty (see “Sharing Talent to Meet Workforce Needs During the COVID-19 Pandemic”).

2. Conduct workforce planning against a budget scenario. SRM leaders can use a workforce framework such as the National Institute of Standards and Technology (NIST) Special Publication 800-181, developed by the National Initiative for Cybersecurity Education (NICE). Such a framework can help leaders self-assess against functions, roles and skills that are applicable for public and private organizations (see “New Security Roles Emerge as Digital Ecosystems Take Over”). This will allow you to organize teams into high-performing and low-performing talent and align essential and nonessential work respectively.

3. Be flexible by limiting nonessential demands. Uncertainties are stressful for everyone, but this is an opportunity for SRM leaders to show leadership skills and seize the opportunity. Pilot this phase for potential cost saving opportunities, but also commit to your employees. This will shape your leadership brand and reputation for years to come.

Evidence

1 IT Key Metrics Data (ITKMD)

Recommended by the Authors

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

Three-Year Roadmap for Cost Optimization

Toolkit: Using Gartner’s Decision Framework and Scoring for Prioritizing Cost Optimization Initiatives

Optimize Risk, Value and Cost in Cybersecurity and Technology Risk
Actionable, objective insight

Position your IT organization for success. Explore these additional complimentary resources and tools for security and risk leaders:

**Webinar**
The Gartner Leadership Vision for 2022: Security and Risk Management
Prioritize your time and energy with top-level guidance based on our data-driven research.

**eBook**
Four Facets of Effective CISO Leadership
Discover how best-in-class cybersecurity leaders tackle their expanding remit.

**eBook**
3 Must-Haves in Your Cybersecurity Incident Response Plan
Improve your organization’s ability to be prepared for a cybersecurity incident.

**Research**
Measure the Real Cost of Cybersecurity Protection
Learn how to make informed cybersecurity risk acceptance decisions.

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

Get actionable, objective insight to deliver on your mission-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

Access more insights for IT leaders
gartner.com/en/information-technology

Stay connected to the latest insights