# How to Manage and Defend Your Security Budget

**Published:** 30 September 2016 **ID:** G00264178
**Analyst(s):** Rob McMillan

## Summary

Many boards now have a clear focus on information security risks. This is not always reflected across the broader organization. Security and risk management professionals must manage and defend security budgets to meet stakeholder expectations of protection.

## Overview

### Key Challenges

Lower-than-expected IT budget appropriations for security often challenge the chief information security officer (CISO) to deliver a level of security that meets the expectations of various non-IT stakeholders such as the board, the executive committee, regulators and shareholders.

While the responsibility to deliver appropriate levels of security falls to the CISO, many times the allocation of budget is influenced heavily by unfavorable peer impressions and limited influence, both at executive levels and throughout the organization.

CISOs sometimes direct disproportionate emphasis to issues of compliance and regulatory focus, resulting in inadequate funding for more urgent concerns related to better security.

The misguided belief that the benefit of security spend is self-evident discourages many CISOs from properly marketing the business benefits, creating unrealistic and counterproductive expectations and reducing the potential for future budget increases.

### Recommendations

CISOs:

Demonstrate to your peers your understanding of the needs of the business and your proficiency as a risk manager, and continually market the benefits of the security program and of your business focus.

Use a strong governance approach to inform and agree on priorities, and to develop realistic budget requirements.

Direct sufficient energies to improving the security posture, countering likely threats and protecting against vulnerabilities while still addressing compliance and regulatory requirements.

Identify the functions necessitated by the organization's specific requirements to discern what work must be done internally and what could be done by external labor.

## Strategic Planning Assumption

Through 2020, only 10% of security budgets will adequately address the convergence of IT, operational technology and the Internet of Things, up from less than 1% now.

## Introduction

The regard for security continues to grow at the highest levels of business — along with opportunities for expanded security budgeting. Fifty-nine percent of CIOs surveyed by Gartner believed that cyber-oriented threats were more of an issue for their business than competitive challenges (see "Building the Digital Platform: The 2016 CIO Agenda" ). Sixty-one percent of organizations say their security budget will increase in FY16, with an 18% average increase. [1] More CIOs rate security in their top three strategic priorities than two years ago, and security is now the seventh highest priority for new technology spending. This intensifying concern for security is resulting in larger appropriations, expanded head counts and new technology acquisitions. But growing budgets come with heightened expectations that will not be met if the CISO does not use proper tactics when interacting with colleagues and executives and when considering specific risks.

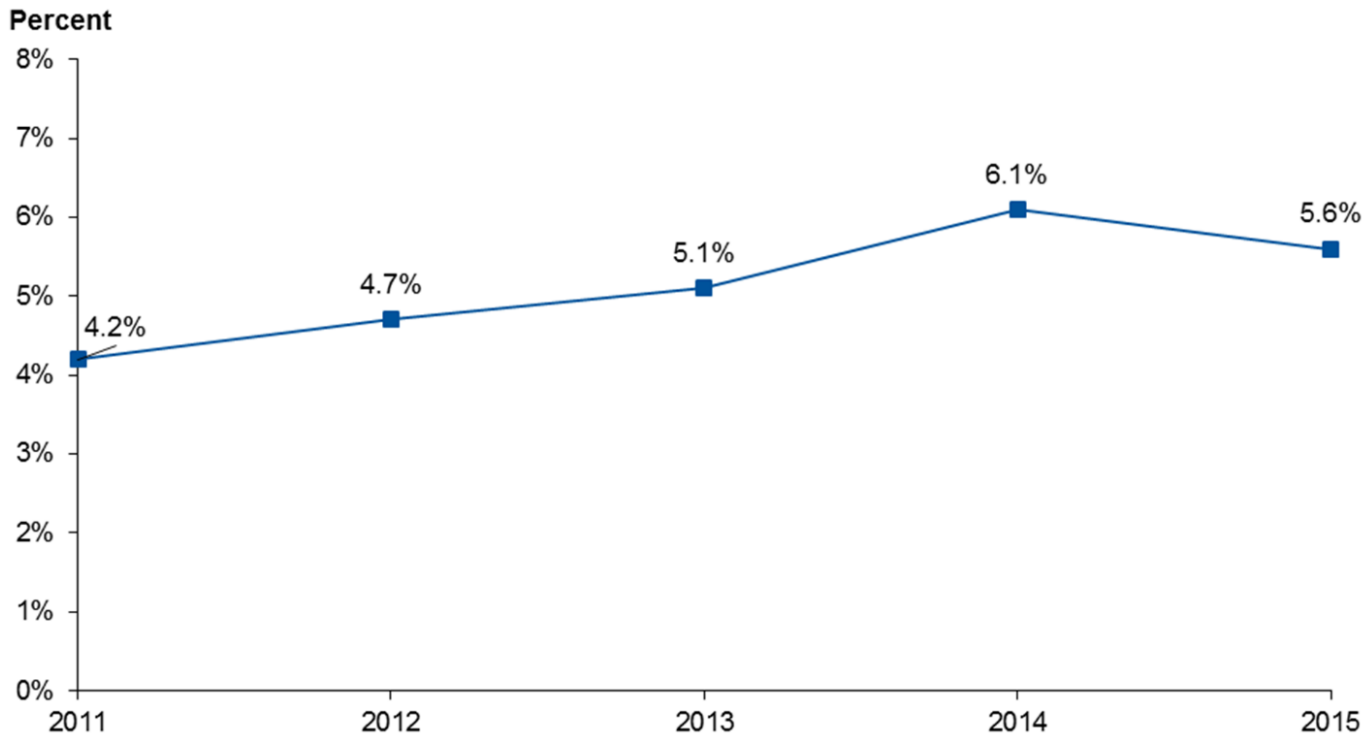
Non-IT executives now sense the grave imperative of security. Security funding must create a balance between the priorities of protection and those of revenue growth and business development. The sensitivity of decision makers to security means CISOs have a willing audience open to supporting security initiatives. To convert this sensitivity into the approval of the best budget for the organization's security — and to the continued success of the CISO — these security officers must position themselves before their peers as business-skilled strategists who can balance the needs to protect with the needs to run the business.

## Analysis

### Go Much Deeper Than Average Spending Figures to Formulate Security Budgets

Current security budgeting throughout most industries is at roughly 5% of a total IT budget (see "IT Key Metrics Data 2016: Key Security Measures: Multiyear" ). Though IT budgets have grown since 2011, funding can easily revert back to underinvestment if CISOs cannot clearly demonstrate the benefits of larger budgets. Despite the widespread optimism for budget growth, Gartner's IT Key Metrics Data shows that a decline in security budgeting has occurred since 2014 (see Figure 1).

**Figure 1.** Total IT Security Spending as a Percentage of IT Spending, 2011-2015




*Source: Gartner IT Key Metrics Data (September 2016)*

To some extent, this decline may be due to the initial alarm raised by high-profile attacks in 2014. However, there are other results that arise from the movement toward digital business. For example, 50% of IT spending is shared with business units outside of IT, and security spending is often spread across various processes and business units, sometimes unevenly and, in many cases, not allocated directly toward explicit security purposes. For organizations in several verticals, the expanding interests in contemporary technologies and services such as mobile device management, cloud, the Internet of Things and virtualization can obscure exactly how an enterprise funds its protections against a range of various threats — or what protections the enterprise requires. Compliance tempts organizations to focus too much energy on checking boxes to achieve regulatory and compliance requirements, leaving other security requirements underfunded.

Leaders often look to match industry norms when creating security budgets. Instead, they should go much deeper. A security budget must address the organization's specific objectives, technologies and risk. (For an overview of due-care security, see "How to Determine If Your Organization Practices Due-Care Security." ) The responsibility to shape such a budget falls to the CISO. Gaining executive support and approval for this budget — which could be larger than past security budgets — falls to the CISO as well.

CISOs are obligated to manage a budget that can expand with the need for new skills as more and more security technologies and procedures become valued tools. To do this, the security leader must appear, in the eyes of their superiors, colleagues and peers as someone keenly perceptive of business objectives and security and technical issues. In the boardroom, in a one-on-one interaction or in a peer forum, a CISO can utilize a range of tactics to convince decision makers that their precise budget will protect the company and allow it to succeed.

**Demonstrate to Your Peers Your Understanding of the Needs of the Business and Your Proficiency as a Risk Manager, and Continually Market the Benefits of the Security Program and Your Business Focus**

At the highest levels of the enterprise, CISOs face an impression problem. The CISO position itself is a relatively new arrival to the executive tier, and the professionals occupying the role find themselves at the lower end of the unstated hierarchy that materializes whenever the company's leaders gather. CISOs struggle to be seen by their leadership peers as more than glorified IT administrators; at worst, their constant caution is taken as obstructionist. Often, many at the C-level see the CISO as the likely scapegoat and sacrificial lamb when a breach occurs or something goes wrong.

Yet the CISO can use their presence at the business's strategic echelon to adjust these negative perceptions, gain a viewpoint of the organization's specific security issues, and advocate for a larger, more tailored budget.

In interactions with their executive peers, the CISO should demonstrate their understanding and support of business objectives and their sensitivity to how security contributes to the company's growth. The risks that a new business initiative might bring should not be described as mere tactical challenges. CISOs should ensure that security is discussed on a strategic level — as a consideration in a new venture but never as a deterrent to a venture. With security practice and budgeting prioritized, resilience can and should be a goal, just as increased revenue, customer conversion or reduced cost might be goals as well.

A CISO can work closely with executives in several areas to help them deal with the constraints under which they must deliver their objectives. For example, the security leader should strive to understand the financial outcomes and preferences that the CIO or CFO is working toward. This awareness can influence decisions such as the technologies or tactics that are adopted to stay consistent with financial accounting policies of the business. If the CFO prefers operating expenditure (opex) over capital expenditure (capex), then the CISO might be able to use SaaS over on-premises technologies as a method to meet that objective. Likewise, a CISO could budget for a managed security service provider (MSSP) as an opex expense, and allocate the MSSP's salaries and wages to other areas.

To develop a deep understanding of each other's objectives and constraints, the CISO should plan to meet regularly with line-of-business executives, even if for 15 minutes, to discuss their objectives and to reinforce security issues. The CISO should research beforehand the colleague's performance criteria, priorities, biases and sensitivities. This research allows the CISO to communicate the agenda or talking points prior to the meeting so both parties know exactly what will be discussed and the overt outcomes that the CISO seeks. The purpose of the meeting is to ensure that the security team is delivering what the business unit needs. Consider the following types of agenda items:

- Metrics or other approaches to demonstrate how security has helped them achieve their successes
- Discussion of what upcoming projects or priorities entail in terms of technology, staff, process, external partners and time frames
- Discussion of what the current or upcoming single biggest concern is for the specific unit
- Scrutiny of what the security team could be doing more/better/different/less

The CISO can use these agenda items to structure the next conversation to show how security is delivering value. They can position successes and, if possible, metrics in the context of the executive's priorities and concerns. When it comes time to make a business case for funding, the

executive should see a clear link between what the security practice is doing and what the executive's unit is doing.

This approach is useful for working with nonsecurity executives to support funding that can be linked directly to business outcomes. It's also useful for helping to support arguments around funding for head count.

Once these meetings have provided the CISO with insight on business unit priorities, the following tactics can be used for budget creation and submission:

**Look for opportunities to generate cost-neutral security gains.** For example, the budget could partially (or fully) achieve the needed security outcome through process changes rather than the acquisition of a new tool.

**Build contingency into the approach.** Without contingency, the effort will have no extra funds to use if the organization has to work with a bad contract-negotiating outcome, unexpected expenses or other adverse events. At the point where this contingency is unlikely to be used, the CISO can redirect it for other purposes, such as providing extra support for other teams in order to build political capital.

**Build concessions into the proposal.** By knowing what ground they can concede, the CISO has room to negotiate and can look for security outcomes that can be achieved by devolving existing effort or by doing something a little differently.

### Use a Strong Governance Approach to Inform and Agree on Priorities, and to Develop Realistic and Reasonable Budget Requirements

A CISO should use a line-of-business-populated governance forum to ensure that budget requirements are appropriate and adequate for the attainment of corporate goals — in other words, that the need for the budget is understood, that it is being applied to the right problems, and that it is sufficient for what must be achieved. This approach can also provide perspective on operational obstacles and areas of obstructed or misdirected funding.

The purposes of this forum are to direct expenditure to the right business needs and most important risks, to ensure that budgets are framed with full knowledge of the consequences of any decisions (to increase or decrease funding), to build political support for budget submissions, and to clear the way should any midlevel management roadblocks arise (see "Security Governance, Management and Operations Are Not the Same" ).

In a periodic gathering of the forum, where governance policies and challenges are expressed, senior staff who are authorized to make decisions independently should expect to address issues with actions. The CISO, acting as host and setting the agenda with input from stakeholders, invites department leaders and operational managers to the forum.

Each time the forum gathers, the agenda should feature action-oriented points and compelling materials that these empowered leaders are prepared to act on immediately. Such agenda points could include:

Collaboration on shared proposals for new technologies, responsibilities or head count for shared security infrastructure

Discussion of material risks, including risks that reach across multiple business units

Policy endorsement and exemption reporting

Presentation of organizationwide metrics to demonstrate support for business imperatives

Building an argument to support projects for new shared security infrastructure

Resolution of a funding conflict

The CISO's further assessment of budgeting should include a review of existing governance and IT operational budgets to inform planning of revised budgets. The leader should plan to review budgets every three to six months with the aim of identifying the most active areas of expenditure; these areas should be the focus of adjustments if required.

### Orient the Security Program to Direct Sufficient Energies to Countering Likely Threats and Protecting Vulnerabilities, as Well as Adapting to Regulatory Changes

According to a survey of Black Hat USA 2015 attendees, top-level security experts feel their concerns don't necessarily match their organizations' security spend. Some 57% said they had concerns about sophisticated targeted attacks but only 26% said such attacks were among the top three spend priorities for their companies. Only 34% said they believed their organization had enough budget to defend itself against likely threats. [2]

Gartner clients often explain that, when uncertain over how much to appropriate for security, they seek to match their security budgeting with average budgeting in their respective industries. Industry behavior can be a valuable guide to companies looking to anticipate risks. However, what really matters is management of your own risks, not the meeting of an average industry figure (see "How to Determine If Your Organization Practices Due-Care Security" ). CISOs can use the emerging volume of "war stories" to good effect in this regard. Clients also admit a large focus on compliance and regulatory adaptation (see "Use Six Principles of Resilience to Address Digital Business Risk and Security" ).

In fact, budget preparation should expand to include several other factors beyond compliance (see "Compliance Is No Longer a Primary Driver for IT Risk and Security" ).

Gartner IT Key Metrics Data (ITKMD) serves as a coarse but useful way to demonstrate whether an organization could be spending more or less on specific security concerns. ITKMD figures tell about a general position in the context of one or more industries, covering one or more sets of costs. The figures offer some guidance around expectation, but CISOs must interpret variances in the context of their specific business situations.

A number of factors must be considered when interpreting whether a business is spending enough or too little:

**Maturity:** If an institution is highly mature, then security costs might be lower than a less mature organization due to operational efficiency. On the other hand, a less mature organization that underspends will also show a low relative figure. If a business is reconstructing security capabilities from scratch — say, for a new digital business initiative — then the CISO should expect the funding requirements to be higher.

**Specific risk appetite and position:** If an organization is culturally ready to accept more risk in the interest of improving business outcomes, then the business may spend less on restrictive controls and more on detection and recovery (see "The Gartner Risk Treatment Model for Digital Business" ). This signifies a different approach than a more protection-oriented posture. The budget may also allocate funds for risk mitigation, such as cyberinsurance or capital allocation.

**Cost structure:** ITKMD is specific about how it structures the cost estimates. However, some costs that have security impacts are not necessarily reflected in the ITKMD. For example, security patches are often applied as part of more general IT operations. This is not likely to be reflected in a security budget. Activities such as prerelease penetration testing can be a grayer area though.

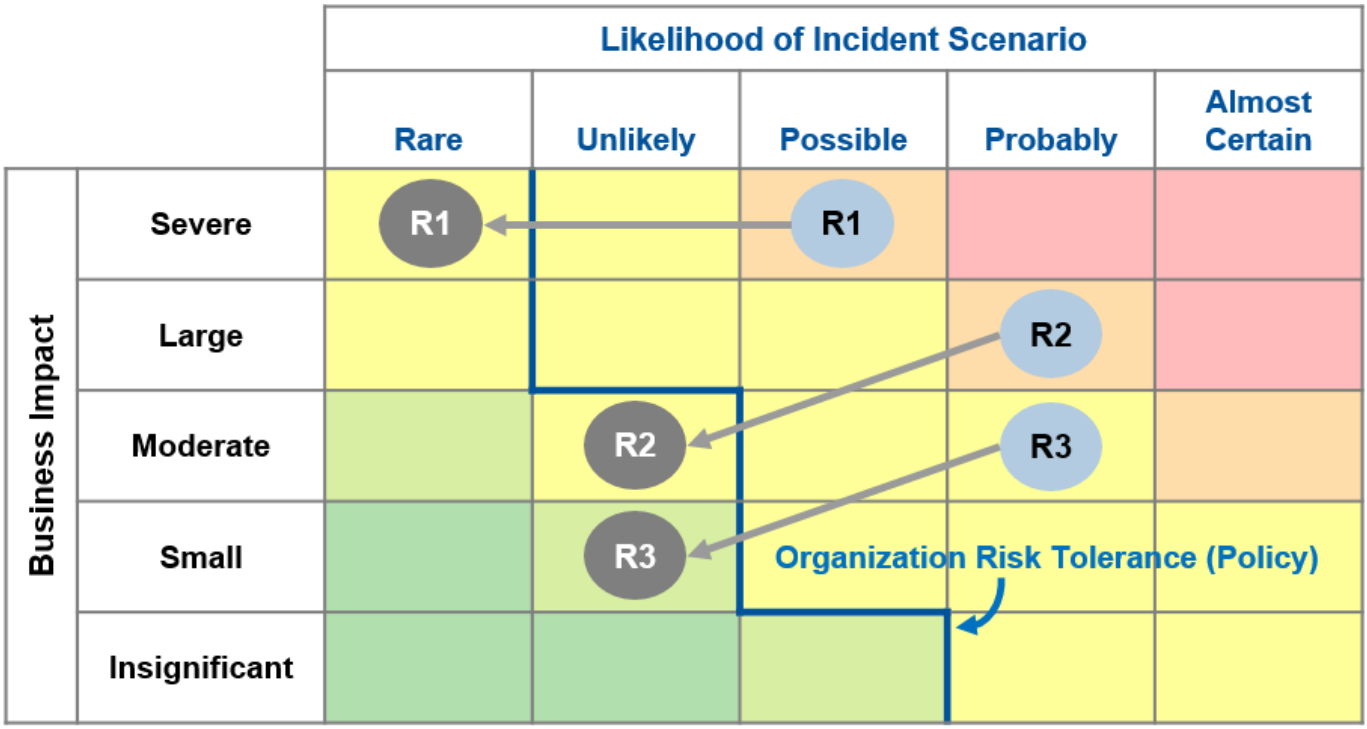
**Negotiating skills:** If a business unit buys the same tools as a peer organization but negotiates a better deal, this expenditure shows up as a lower spend than initially expected based on existing business guidelines.

When seeking to position themselves among their peers as a source of understanding and support to larger business objectives, the CISO should help decision makers understand their current risk position and the relationship between funding and the management or mitigation of those risks. An accountability model is useful here, linking specific risks to specific executives. The CISO should express how security deficiencies link to those risks and how addressing these deficiencies does not deter — and in some cases advances — business performance. Risks are often ignored in traditional value management. Addressing them can add new value.

See "The Gartner Business Risk Model: A Framework for Integrating Risk and Performance" and "Toolkit: Board-Ready Slides for Cybersecurity and Technology Risk" for illustrations and more perspective on these issues.

At times, the CISO is offered funding but at a lower level than what is sought. Figure 2 shows how a shortfall in funding may have a material, negative impact on the reduction of a particular risk, since the diagram shows a relationship between the proposed work program and the reduction of the risks. If this situation arises, the CISO could counter the reduced funding limit by showing which risks would not be sufficiently reduced, or by tactfully asking for direction about which risks should be left outside tolerance — as depicted in Figure 2. (For an overview of a funding narrative, see "Board-Ready Slides for Cybersecurity and Technology Risk: Sample Narrative — Funding Request." )

**Figure 2.** Assessing Risk Tolerance




**Legend**


| | |
|---|---|
| R1 | Loss of product and manufacturing secrets due to disclosure of sensitive intellectual property. |
| R2 | Loss of consumer confidence and sales due to audit failure. |
| R3 | Degradation of production volume due to manufacturing interruption. |

Example

*Source: Gartner (September 2016)*

**Identify the Functions Necessitated by the Organization's Specific Requirements to Discern What Work Must Be Done Internally and What Could Be Done by External Labor**

When a CISO is making the case for head count, he or she should map the critical functions that must occur throughout the organization's security responsibilities.

The number and complexity of tasks in the breakdown structure depends on the size and complexity of the organization. Examples of these functions are listed below (see "Toolkit: Security Capabilities Framework for SMBs" ):

- Policy and compliance
- Audit issue remedy
- Awareness
- User provisioning/deprovisioning
- Security patching
- Endpoint configuration
- Firewall configuration

Log monitoring/response

External threat monitoring

Once these tasks have been mapped, the CISO should quantify the effort required to perform these functions adequately. Remember that staff will also be sick, take vacation, or have days in which some tasks will take priority and may take unexpectedly long periods of effort. For example, a particularly difficult-to-resolve audit issue or the emergence of a security incident could easily change the estimates for duration.

The CISO should then assess the extent to which this work is being done. Remember that the work might be performed in the security team or it could be performed by others. Patching is a classic example; security patches can often be installed by IT operations. Regression testing can be an important and time-consuming exercise, and in larger organizations would be a significant work item in itself. Log monitoring could be performed by an external supplier.

A rule of thumb is that functions that require knowledge of the internal culture of the organization (for example, policy development) should be made by internal staff.

The CISO should look at the work items for which less than the expected effort is occurring — or where even no work is being performed. They should then question the impact on the organization in each case. Is this a potential risk that can be accepted? If not, then some type of funding will be required to meet the requirement, whether it is internal full-time equivalents (FTEs) or some type of outsourcing.

It will be easy for executives to state that the security practice will just have to do the best that it can with the available resources. The CISO should make sure that the executive team is aware of the work that won't be done and ensure that this links in with the risks in the risk register, as discussed above. If the neglected work doesn't link with a risk that would exceed the company's risk tolerance, then the CISO does not have a strong case for the extra head count.

## Evidence

[1] Survey conducted by Gartner from May 2016 to July 2016, among 512 respondents in eight countries: Australia, Canada, France, Germany, India, Singapore, the U.K. and the U.S.

[2] M.Cox. "Black Hat Attendees: Enterprise Security Wastes Most Budget and Resources." (http://www.channelbuzz.ca/2015/07/black-hat-attendees-enterprise-security-wastes-most-budget-and-resources-14139) ChannelBuzz.ca. 15 July 2015.

---