Secureworks®

WHITE PAPER

Smart Spending: 6 Tips for Allocating your Cybersecurity Budget

A Guide to Efficient Cybersecurity Spending

Every business has unique operational requirements, and that's certainly true when it comes to budgets. With many IT budgets increasing to handle a variety of factors, such as digital transformation and a shifting economy, more businesses are revaluating their cybersecurity budgets. According to the ESG 2020 Technology Spending Intentions Survey:[1]

- 62% of organizations will increase cybersecurity spending in 2020, while another 36% will keep cybersecurity budgets flat. Technology organizations are most likely to increase spending (73%), followed by manufacturing (68%), and retail/wholesale (67%).
- 40% of survey respondents identified cybersecurity as the business initiative that will drive the most technology spending in their organization over the next 12 months.

62%

of organizations will increase cybersecurity spending in 2020.

40%

of survey respondents identified cybersecurity as the business initiative that will drive the most technology spending over the next 12 months.

These data points indicate that cybersecurity is recognized as a business imperative across industries, which is encouraging as businesses grapple with an increase in cybersecurity threats – in part due to a growing remote workforce. But a bigger budget doesn't mean an infinite budget, and it's critical that business and security leaders spend their cybersecurity dollars as efficiently as possible. This paper will provide a framework for allocating cybersecurity budget efficiently to make the greatest impact across your unique business environment.

Is the Budget Inherited, or Brand New?

Many security leaders will inherit a security budget, but some will be able to build their budget from the ground up. Determine whether cybersecurity is a new budget line item, or if it's something that has already been funded by previous leaders. If the budget has already been funded and is not being built from scratch, identifying inefficiencies is especially important. However, in both circumstances, the guidelines for building a budget are the same. If the business in question is building from scratch, it won't be as important to identify already-existing inefficiencies, but each of the following points will be important to consider in preventing inefficiencies. If the budget already exists, the rest of these tips can help identify and cut waste and build a more streamlined program.

[1] ESG, 2020 Technology Spending Intentions Survey

6 Tips for Efficient Allocation

Although every organization is unique, these six tips for efficient budget allocation can help leadership form the framework for building a budget and communicating the changing needs of the organization:

1. Understand the Business Landscape

Just as security leaders must understand the threat landscape, it's equally important to understand the business landscape of your organization and design a security budget around that. Is the organization more focused on mergers and acquisitions, lift and shift, or innovating new products? Tailor the cybersecurity budget needs to what drives the organization.

Tackling this step means identifying an organization's unique risk tolerance and capacity to spend in support of a company's level of risk. But how is that determined? It's vital to understand the culture of the organization as the budget is being built. If a company is heavily focused on mergers and acquisitions, the cybersecurity budget must be more fluid to handle the unknowns – we don't know what company might be acquired, the size of the acquisition, or the shape of the new cybersecurity program that must be addressed after the merger.

Organizations must determine whether their budget is static or if it can increase throughout the year. In either case, building an allowance for variance into the budget is critical to maintain flexibility and adjust to changing needs before requesting additional budget. When building a program, you can't foresee every issue that may arise – changes to the economy, new regulatory requirements, or that you may need to spend slightly more on X versus Y to get the best results. With variance built in, organizations can adjust as needed without a new budget request, which may be frowned upon and/or rejected.

It's also important to remember that leaders can and should consult with other departments, whether that's technology leaders or peers, to ask how they handle variance in their budgets as a guideline.

2. Understand the Threat Landscape

This will be unique to the industry and organization, but it's critical to understand the events, incidents, and potential breaches that the business may face and how to best mitigate the risk of them happening. Access to threat intelligence is a key way for organizations to accomplish this. In particular, third-party security vendors can be helpful with providing threat intelligence monitoring and research. Vendors also provide insight into incidents happening in similar environments that may reveal threat actor activity and potential threats your organization or industry may face.

3. Monitor and Measure

Creating a program with strong measurement and key performance indicators (KPIs) will help leadership determine how effectively the budget is being spent based on results. This data can then be used to help cybersecurity leaders make the case for more budget as needed when the new fiscal year arrives. So which KPIs are most useful for organizations to monitor?

Patch Management: As the remote workforce grows, this is an important KPI to have in place. It shows when there's a shift in asset management, and when operating system upgrades are needed.

User Awareness and Training: Training company employees how to identify threats they can help control, such as phishing, is an important part of the overall security investment. It also helps demonstrate that the team is doing its due diligence, and if an attack does happen, it was because the threat actor was particularly skilled and not that the cybersecurity program didn't have checks and balances in place.

Events and Incident Management: This shows what types of events are happening on a monthly basis, and how many were connected to breaches. Not every event is an incident, and not every incident is a breach in which the C-suite must be warned, so these need to be monitored and measured separately.

Audit Compliance: It's important to regularly assess your organization's adherence to regulatory guidelines and policies. An audit can also evaluate the strength and thoroughness of your internal security controls to protect the confidentiality and availability of data. These findings can translate to dollars for the budget, so it's important to measure this category as well.

4. Determine if the Program is Risk-Based or Tactical

Although every organization must determine what "smart spending" looks like to fit its own unique culture and values, a key guideline is to spend the cybersecurity budget like it's your own money. This will help stop leaders from overspending by identifying if it's an investment that really needs to be made. It's also important to ask if your decisions are reactive, or if they are driven by an incident, a regulatory compliance need, or a future need. This can help determine what is tactical versus what is risk-based and helps program managers know where the money is going.

If a cybersecurity program is largely reactive, we can expect to see more inefficiencies as the mindset is about stopping the threats and using whatever "bandage" is available to do so. A more strategic mindset is needed to identify where the threats are coming from, how to stop them, and how to deploy a strategy to identify and stop threats before they become a critical problem.

Cybersecurity budgets should be focused on proactive spending, not reactive spending. What does that mean in practice? A good first step in determining how to spend proactively is a security awareness audit for all employees – what general knowledge do a company's employees have about phishing, individual network security, and other security concerns that can help keep threat actors out in the first place? Employee training is not as valued as it should be from a resourcing and budgeting standpoint – many organizations see cutting training as a savings, but they will fall behind the curve when it comes to practicing basic cyber hygiene.

5. Decide Whether the Program Should Be In-House or Managed Externally

People costs make up a significant portion of the security budget, but a managed security partner can help streamline the budget by adding efficiencies regarding knowledge-sharing, training, and reporting.

Cybersecurity budgets can be broken down into three categories: people, technology, and cyber insurance.

People – This includes the cybersecurity staff you already have in the organization, the staff you need to hire, as well as managed partner costs. For internal hires, this line item should include not only salaries and benefits, but initial training, ongoing maintenance training, and backfill. A managed partner could feasibly take the place of certain new hires within the organization, so organizations must weigh the costs and benefits of each to make the decision that's right for them.

Technology – Technology that organizations need to allocate funds for include endpoint protection, encryption, protection of data through multi-factor authentication, SIM and log management that monitors how you are storing and analyzing data, and asset management. Depending on the organization, asset management may fall under IT, so it's important to determine ownership and factor into the budget accordingly.

Cyber Insurance – This is a relatively new factor, but mid-enterprise and larger organizations are implementing cyber insurance more and more by default. The ownership of this line item is typically either general counsel, legal, or cybersecurity leadership, which must be considered when building a budget.

Budget inefficiencies can also be traced to having multiple cybersecurity vendors. As businesses build their cybersecurity budget strategy, it's important to assess what vendors are actually providing, if there is any overlap with what other vendors are providing, and if there is a single vendor that offers all the services under one umbrella. Think about this concept from a knowledge-sharing perspective – if multiple vendors are performing multiple functions, it's highly unlikely that they are communicating and sharing their findings with one another. A single vendor encourages greater knowledge-sharing and needs less onboarding time, which positively impacts the bottom line.

6. Determine the "Big Ticket" items

The transformational priorities of every organization are different, but might include a shift to the cloud or an overhaul of current systems. Once those are determined, leaders can decide what new infrastructure needs to be secured, if any. Security must be a big part of these transformational projects and they must be reflected in the security budget.

It's also critical to know what the ROI will be for a new investment, and how to communicate engagement value to leadership. As previously mentioned, a security vendor can not only help reduce budget inefficiencies but can also help your organization spend smarter if they're preventing or quickly remediating cyber incidents, filling resource gaps, and providing threat intelligence that informs your organization's security strategy.

Organizations should also factor in brand value when determining how to spend proactively-- not only on big ticket items, but for the entire security program. If a brand is worth $10M, it makes perfect sense to spend $100,000 on security to help protect the brand. If an organization is unsure of its worth, it may seem like too large of investment – in this case, a brand value exercise is a key step in determining the appropriate level of spending for the overall cybersecurity program and individual initiatives.

Bonus Tip: How to Allocate Budget Increases

You've built your budget and feel confident that it's resulted in a strong program with little waste. So how can you start planning to request a budget increase, or implement an increase that hasn't been formally requested? When requesting a budget increase, or determining what to do with additional funds, it's important to consider the maturity of your organization's security program. If the program is where it needs to be, then spending should largely be allocated to keep the program running. The business will have incidents, but with a strong incident response plan and incident response partners, the team can focus on maintaining the program. The maturity of the program can be proven out by the KPIs being measured.

If an organization is starting from greenfield, then having an 18-month, three-year and five-year roadmap will help drive the budget conversation: year one and two will be focused on designing and building, while years three and four will be more operational. From that point forward, the focus is on maintaining the strong program that's been built. This will help leadership understand why the cost is going up, and that at some point during the roadmap the spend will level off, avoiding any surprises regarding the budget.

The Bottom Line

Building an efficient cybersecurity budget can be a complex process with multiple factors and outside influences to consider. But with this framework as a starting point, cybersecurity leaders can spend with confidence knowing that the most important needs of the business are being met at every turn.

With this framework as a starting point, cybersecurity leaders can spend with confidence knowing that the most important needs of the business are being met at every turn.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp