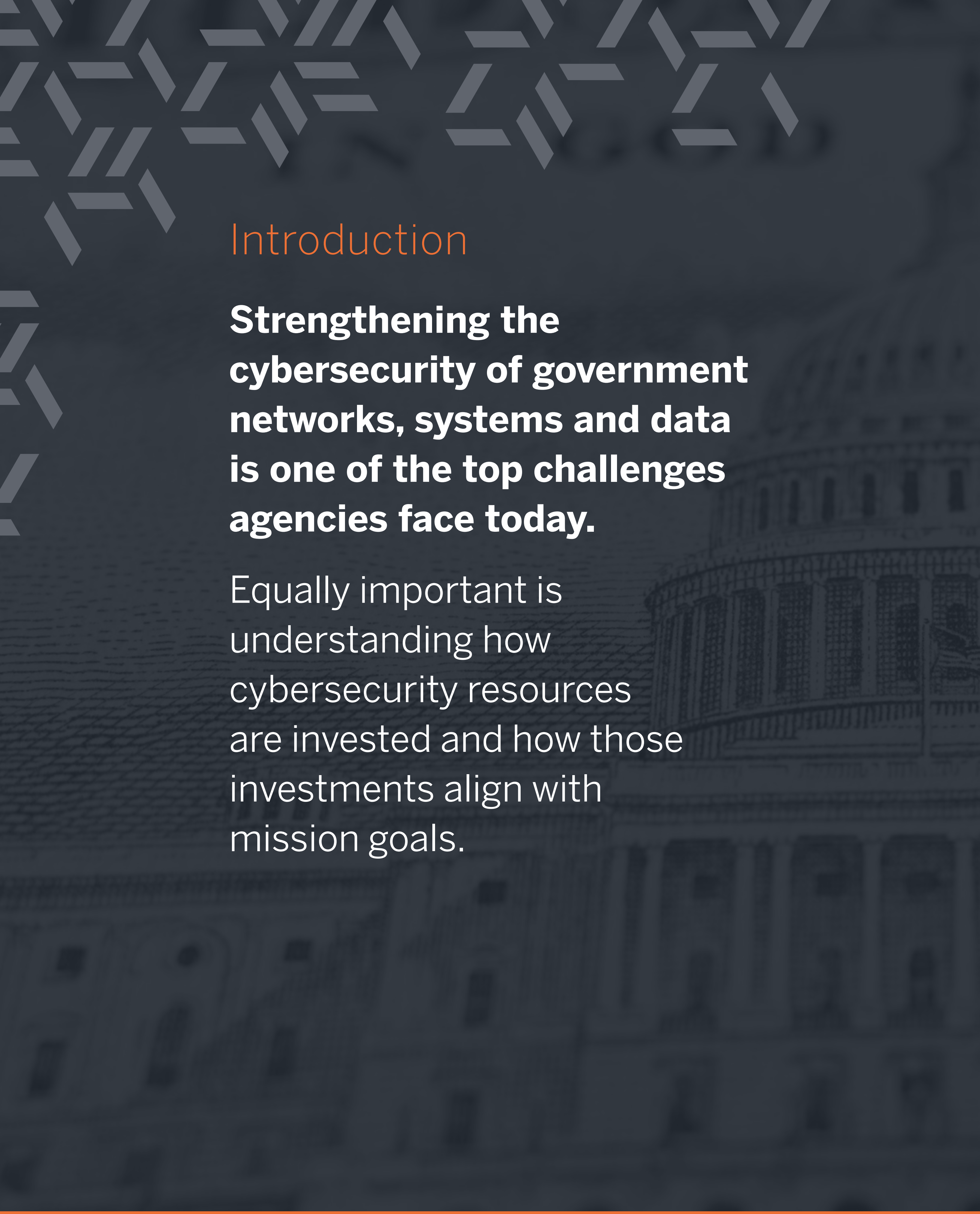
Managing Cybersecurity Spend – Value & Outcomes

RESEARCH BRIEF

govloop



Introduction

Strengthening the cybersecurity of government networks, systems and data is one of the top challenges agencies face today.

Equally important is understanding how cybersecurity resources are invested and how those investments align with mission goals.

The president's fiscal 2019 budget includes $15 billion for cybersecurity-related activities, a $583.4 million or 4.1 percent increase above the fiscal 2018 estimate.

But that number alone doesn't tell the whole story. Due to the sensitive nature of some activities, not all cybersecurity funding is included in that figure.

For many agencies, accounting for all cybersecurity spending is a challenge, in part because existing methods in place to track that spending don't provide a comprehensive view or the necessary granularity.

There is a concerted effort to empower government executives to make data-driven decisions, specifically around IT investments, which includes cybersecurity. This standardized approach, known as Technology Business Management (TBM), is gaining traction in the federal government and is expected to be implemented governmentwide by 2022. TBM provides a set of best practices for categorizing IT costs, technologies, resources, applications and services, and for effectively communicating what business value IT investments actually provide.

To better understand how agencies are currently tracking their cybersecurity spending, GovLoop partnered with Apptio, which provides a FedRAMP-certified, cloud-based software and an on-premises offering for managing the business of IT. In the following pages, we analyze the results of a survey of more than 100 public-sector employees who are involved in finance and IT at their agencies. They were asked about their agency's ability to accurately track cybersecurity spending, top challenges for managing cybersecurity spending and if those dollars align with the Cybersecurity Framework developed in part by the National Institute of Standards and Technology (NIST). We also share insights from Bob Carter, Vice President of Public Sector for Apptio, who provides best practices for improving the way agencies manage spending and ultimately improve cost visibility for cybersecurity.

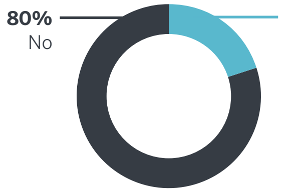
How Are Agencies Managing Cybersecurity Spending Today?

Generally speaking, cybersecurity funding represents a small portion of an agency's overall IT budget. To determine how well agencies are managing that spend, GovLoop surveyed 113 public-sector employees about the approach their agency is taking to track cybersecurity spend, the top challenges they are facing and their plans for future cybersecurity spending.

Eighty percent of those surveyed said they do not know what their agencies spend on IT today (See Figure 1). "A lot of folks know their budget, but they don't know their costs," Carter said. "That's part of the problem itself, getting their arms around the actual cost and where the money is going."

FIGURE 1

Do you know how much your agency spends on information technology?



According to the President's Management Agenda, "The FY 2018 President's Budget reported 84% of the total Federal IT budget categorized as 'other,' as opposed to being clearly tied to a specific IT category of spend. This lack of granularity makes it difficult to baseline federal investments and show the public whether [the] government is spending taxpayer dollars effectively in order to drive the large scale change needed to improve business transformation and citizen services."

As a subset of the federal government's $90 billion IT budget, cybersecurity spending is often disjointed, Carter said, highlighting three key reasons why that's the case.

1. Often, agencies don't use a standard method like TBM to model or account for cybersecurity costs. For example, they may not track costs that come with securing an application, or those costs may get labeled as IT overhead.

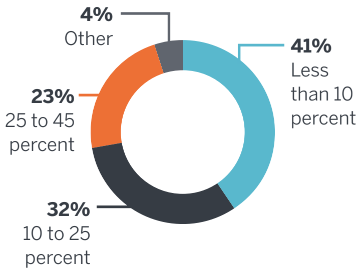
2. Although agencies have been required to adopt the NIST Cybersecurity Framework (CSF), there is not clear guidance on how they should use the framework as a means to track spending.

3. As noted in the President's Management Agenda, there are some gray areas where it isn't clear how to categorize certain cybersecurity costs. This prevents agencies from having a transparent and accurate view of what they are spending.

For the other 20 percent who said they know what their agency spends on IT, we asked them to estimate how much of their IT budgets go toward cybersecurity, which includes tools, processes and personnel (See Figure 2).

FIGURE 2

How much of your IT budget do you estimate is spent on cybersecurity (this includes tools, processes and personnel)?



Roughly 18 to 22 percent of the federal IT budget is spent on cybersecurity, Carter said, with the caveat that some spending is classified and nearly impossible to track. That number aligns with what we heard from 32 percent of respondents, who said cybersecurity accounts for 10 to 25 percent of their agency's IT budget. Another 41 percent said that cybersecurity is less than 10 percent of the IT budget.

The size of the agency and amount of the overall budget are factors that impact how much agencies spend on cybersecurity. But those aren't the only factors to consider, Carter said. How agencies categorize spending also determines how they report it. For example, one agency may group all IT network costs together, but they don't take into account what within the network could be considered cybersecurity spend. Likewise, for software application costs, agencies should determine what within the applications is considered cybersecurity spend.

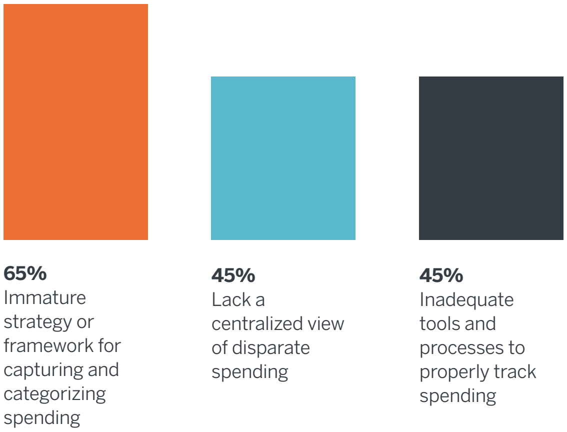
Agencies are taking steps to improve how they categorize and track IT spending, but with any change comes inherent challenges.

Top Barriers to Better Management of Cybersecurity Spending

We asked respondents what their top challenges are when it comes to managing cybersecurity spending (See Figure 3).

FIGURE 3

What are the top challenges you face when it comes to managing cybersecurity spending?



The greatest challenge — noted by 65 percent of respondents — is an immature strategy or framework for capturing and categorizing spending. That was followed by lack of a centralized view for disparate spending and inadequate tools and processes to properly track spending — both of which were identified as top challenges by 45 percent of respondents.

“Overall, people need a repeatable, sustainable and automated way of capturing and managing all these costs,” Carter said. “It’s the old adage: You can’t manage what you don’t measure. So measuring all these costs is key.”

For example, the process that agencies use to select, manage and evaluate IT investments, known as capital planning and investment control (CPIC), does not provide information at the account level, and it doesn’t capture non-IT cybersecurity investments, according to the president’s fiscal 2019 budget request. There are numerous programs that enhance national and federal cybersecurity but are focused on areas such as standards, research and the investigation of cybercrimes rather than specific technical capabilities.

Because federal funding is often allocated by programs and offices, it’s hard to gain a centralized view of how money is budgeted and spent. That means mission programs and IT and finance departments aren’t always planning and making decisions based on the same data. When these offices are not operating in harmony, critical cybersecurity investments may be overlooked, underfunded or not adequately supported.

Respondents also cited inadequate tools to track cybersecurity spending as a challenge. But that can also pose a security risk, Carter said. “A lot of these handcrafted solutions are also subject to security problems. That’s the ultimate irony. Here we’re talking about cybersecurity costs, and yet you start building these one-offs, and the data managed and maintained within these systems are subject to security risks, such as not being encrypted and secured during data transfer.”

In terms of processes, many agencies are still using spreadsheets to manually track spending, rather than automating that task, Carter said. More people and spreadsheets are not going to solve the budget challenges agencies face with variance issues and little visibility into how money is being spent. The issues are compounded when cybersecurity spending must be tracked across multiple agencies that are sharing services.

> *“It’s the old adage:* ***You can’t manage what you don’t measure.*** *So measuring all these costs is key.”*
>
> Bob Carter, Vice President of Public Sector for Apptio

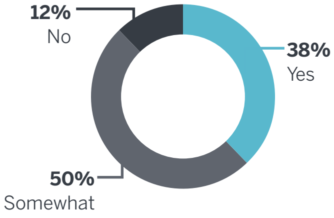
Tracking the Cost of Cybersecurity Shared Services

Governmentwide, there's a concerted effort to use shared services to improve IT services and reduce procurement costs. As the number of agencies sharing a service increases, it's important that those customer agencies understand how much those services costs and what they are paying for.

Part of the challenge is that agencies can't provide a centralized view of cybersecurity spending to their shared services customers if they lack that level of transparency themselves (See Figure 4). Most respondents — 50 percent — have a somewhat centralized view of cybersecurity spending across shared services customers. Thirty-eight percent said they do have a centralized view, and 12 percent said they do not have a centralized view.

FIGURE 4

Do you have a centralized view of cybersecurity spending across shared services customers?

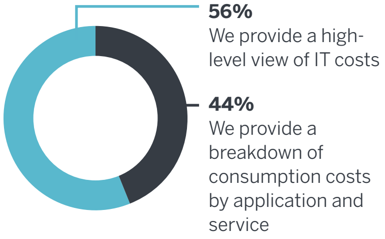


One of the benefits of understanding shared services costs is that agencies and their customers can accurately determine if the cost of a federal shared service is competitive, compared with what they would be paying elsewhere. Agency customers that are considering migrating to as-a-Service options, for example, need to understand what they are currently paying for cybersecurity services. However, the way agencies are billed can make that exercise difficult.

When asked how shared service customers are billed, 44 percent said they provide their customers with a breakdown of consumption costs by applications and services (See Figure 5). Fifty-six percent said they provide shared services customers with a high-level view of IT costs.

FIGURE 5

Which of the following describes how you bill shared services customers?

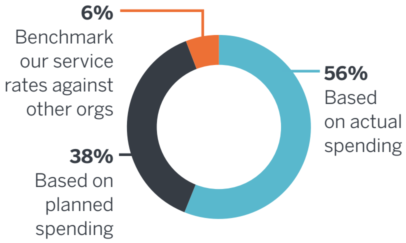


"Most people are looking for true numbers, true costs and true consumption figures," Carter said. Agencies should strive to have consumption-driven cost models that transparently identify what agency customers are spending on cybersecurity, so they can charge them accurately for the services they used.

When asked how they set service rates for customers, 56 percent said those rates are based on actual spending data (See Figure 6). Thirty-eight percent said those rates are based on planned spending, and 6 percent said they are based on benchmarks against other organizations. Understanding the fee structure for cybersecurity services is not an agency-by-agency issue but one that must be detailed in the federal budget. Agencies should also consider how their rates can either drive or deter adoption of a particular service.

FIGURE 6

How do you set service rates for shared services customers?



"The budget is also required to include an analysis of fee-based cybersecurity costs as well as gross and net appropriations or obligational authority and outlays," according to budget documents. "Agencies have not historically reported their cybersecurity budgets in this manner, and OMB continues to work with the broader federal community to capture this information in a way that is helpful to both agencies and Congress."

Agencies are in the early phases of gaining greater transparency of cybersecurity shared services costs, Carter said. "I think folks are trying to get their arms around their cybersecurity spending and being more accountable. Depending on what branch of the government you're talking about, some are a lot more advanced than others. For example, Defense and Homeland Security departments are more advanced than others."

In the next section, we'll discuss how the NIST Cybersecurity Framework can be used to better manage cybersecurity costs.

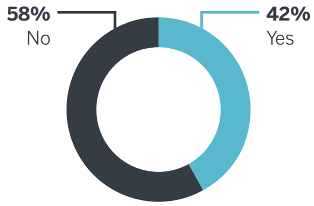
Cybersecurity Spending and **the NIST Framework**

One way for agencies to maximize their cybersecurity budgets is to align spending with the CSF, Carter said. Today agencies are at different levels of adopting the framework, following a 2017 presidential executive order mandating that they implement it.

Of those surveyed, 42 percent said they are using the CSF, and 58 percent are not (See Figure 7).

FIGURE 7

Is your agency leveraging the NIST CSF?



But Carter expects that number will increase over time as agencies work to comply with the executive order.

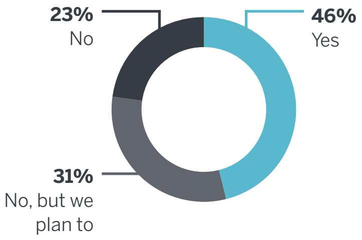
"Future years will array agency cybersecurity information against the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)," according to the president's fiscal 2019 budget. "The incorporation of the Cybersecurity Framework, to which cybersecurity performance metrics and risk management assessments are already aligned, will provide a more structured manner for discussing Federal cybersecurity budgets and how they strategically address areas of noted risk."

The benefit for agencies is about more than compliance, encompassing an improved way of managing cybersecurity spending. The five categories outlined in the framework — Identify, Protect, Detect, Respond, and Recover — give agencies a common outlook for measuring their cybersecurity investments and managing risks.

Of those who said they are using the CSF, 46 percent said they are measuring their cybersecurity spending according to the five functions of the framework (See Figure 8). Thirty-one percent said they are not using the framework but plan to, and 23 percent are not using it at all.

FIGURE 8

Are you measuring your cybersecurity spending according to the five functions of the NIST CSF?



Here's a practical example of how the CSF can help federal agencies. Let's say most of your agency's cybersecurity funding is going toward the Identify function, which entails recognizing cybersecurity risk to systems, people, assets, data and capabilities. But have you considered whether your agency has enough money to respond to an incident or recover from one? If there is a service attack, can your agency quarantine computing services, respond accordingly and recover?

"If you don't have enough money in these other categories, you might be vulnerable, or you might be blindsided after the fact because you didn't have visibility into how resources are being spent," Carter said. "We strongly recommend that agencies understand their overall costs and incorporate the NIST framework into their financial categorization to manage and know where their money is truly going."

Using the framework to properly group cybersecurity spending aligns closely with a set of best practices that agencies are starting to use to track IT spending in a more granular and transparent way. We discuss this methodology in more detail in the following section.

How Agencies Can Better Manage Cybersecurity Costs With TBM

There's a standard approach to managing IT spending that is being promoted through the President's Management Agenda and through guidance from the Office of Management and Budget. It's called TBM, short for Technology Business Management.

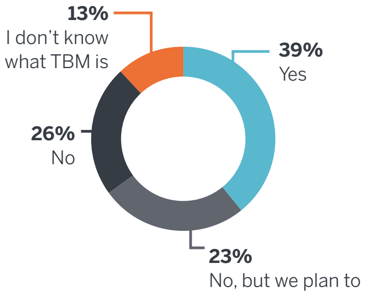
In spring 2017, OMB directed agencies to begin adopting elements of the TBM framework — an open-source standard for IT costs. "This will provide more granularity in IT spend based upon a taxonomy broadly accepted across both private and public sector organizations," the President's Management Agenda noted.

By 2022, federal agencies and their vendors should be tracking and communicating the value of IT investments using TBM. "It is the discipline in which one should categorize your IT investments, your cybersecurity investments, your labor investments, even your enterprise business investments, into different categories," Carter said. "And ultimately you want to get a higher-level view — by application, by service, by program — and then further understand what is the cybersecurity portion of each of these deliverables or services."

The good news is 39 percent of respondents are using TBM to track financial investments around cybersecurity (See Figure 9). Twenty-three percent are not but plan to, and 26 percent are not using TBM at all. Thirteen percent don't know what TBM is. There is certainly room for more education around TBM, especially in the government finance and procurement communities, where TBM terminology is still taking root.

FIGURE 9

Are you leveraging the TBM Framework to track your financial investments around cybersecurity?



A lot of cost data in the federal government is siloed, which makes a standard approach like TBM vital for normalizing, automating and mapping data into categories that can be rolled up into an accurate and shared view of spending across the agency. In order for agencies to scale and automate the budget tracking they do today, they need a repeatable and sustainable process.

There's data in the President's Management Agenda that shows how early adoption of TBM drastically improved agencies' ability to track IT spending with more granularity and clarity. The percentage of IT costs labeled as "other" dropped from 84 percent to 34.7 percent. The expectation is that having this type of detail will help agencies make tough decisions like where to spend limited dollars, whether a move to the cloud makes sense for a particular system and areas that may be ripe for cost savings.

Speaking at a July TBM Public Sector Summit in Washington, D.C., Federal Chief Information Officer Suzette Kent acknowledged that TBM adoption won't be a simple task for many reasons, including the fact that agencies are at different places in terms of understanding their specific IT costs. She also said TBM will not be a check-the-box exercise but rather focus on reframing how government serves the public.

"What we're moving to is an environment that is more data-driven, more transparent, [one in which] we have clarity of where we're putting taxpayer money, but ***more importantly we have visibility to the outcomes that have been achieved*** *and that we can show those through data at any point in time," Kent said during the event.*

Some of the challenges agencies will face when adopting TBM are also cultural, Carter said. Some people are resistant to change, so it takes education and exposure to help them understand the value of moving beyond spreadsheets to embracing TBM. TBM is all about value and outcomes. Compliance is a high-value byproduct of TBM.

Are You Planning for Future Cybersecurity Spending?

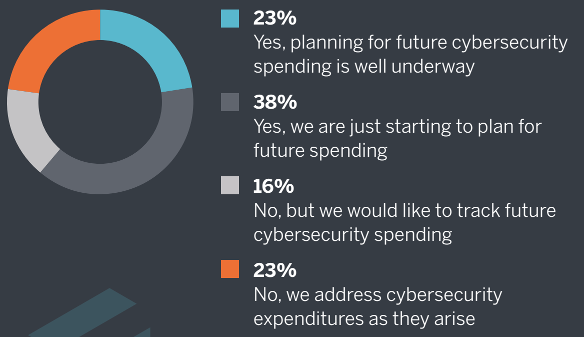
Another benefit of using TBM and the NIST Cybersecurity Framework to manage cybersecurity spending is that they enable agencies to adequately plan for future needs. We asked respondents if they are budgeting for cybersecurity spending in future years (See Figure 10).

Twenty-three percent said that planning for future cybersecurity spending is well underway. Thirty-eight percent said they are just starting to plan for future spending, and 23 percent said they address cybersecurity expenditures as they arise.

Planning for future spending is a best practice when it comes to budgeting for cybersecurity or anything else, Carter said. “It allows you to reduce a lot of the variance between your budgeting, planning and actual spending. At the end of the day, you would like the spending, budgeting and planning sides of the agency to have one view, so everyone can collaborate, communicate and use the same language when looking at costs.”

FIGURE 10

From a budgeting and planning perspective, are you budgeting for cybersecurity spending in future years?



How Apptio Helps You Manage Cybersecurity Spending

Apptio pioneered the Technology Business Management discipline and is the premier provider of TBM SaaS applications.

Through its TBM methodology, Apptio transforms the way IT runs its operations and makes decisions. Using cloud-based applications, IT leaders manage, plan and optimize their technology investments across on-premise and cloud solutions. With Apptio, IT leaders become strategic partners to an agency’s business units by demonstrating value of IT investments, accelerating innovation and shifting their technology investments from running the business to digital innovation.

By joining forces with a partner like Apptio, agencies can develop a strategy for adopting the TBM framework and determine what process changes and capabilities must be in place to better manage and communicate the value of IT.

Apptio automatically aggregates, cleanses, and establishes relationships across large amounts of data from disparate financial, operational, and vendor invoices, and maps that data into the standard TBM IT cost model. With Apptio, IT can shift 6 to 8 percent of spending into innovation to strategically align with the broader goals of the agency.

Apptio’s TBM solutions align technology investments to mission priorities, engage mission stakeholders to drive accountability and value, and optimize and increase efficiency of hybrid IT resources.

Conclusion

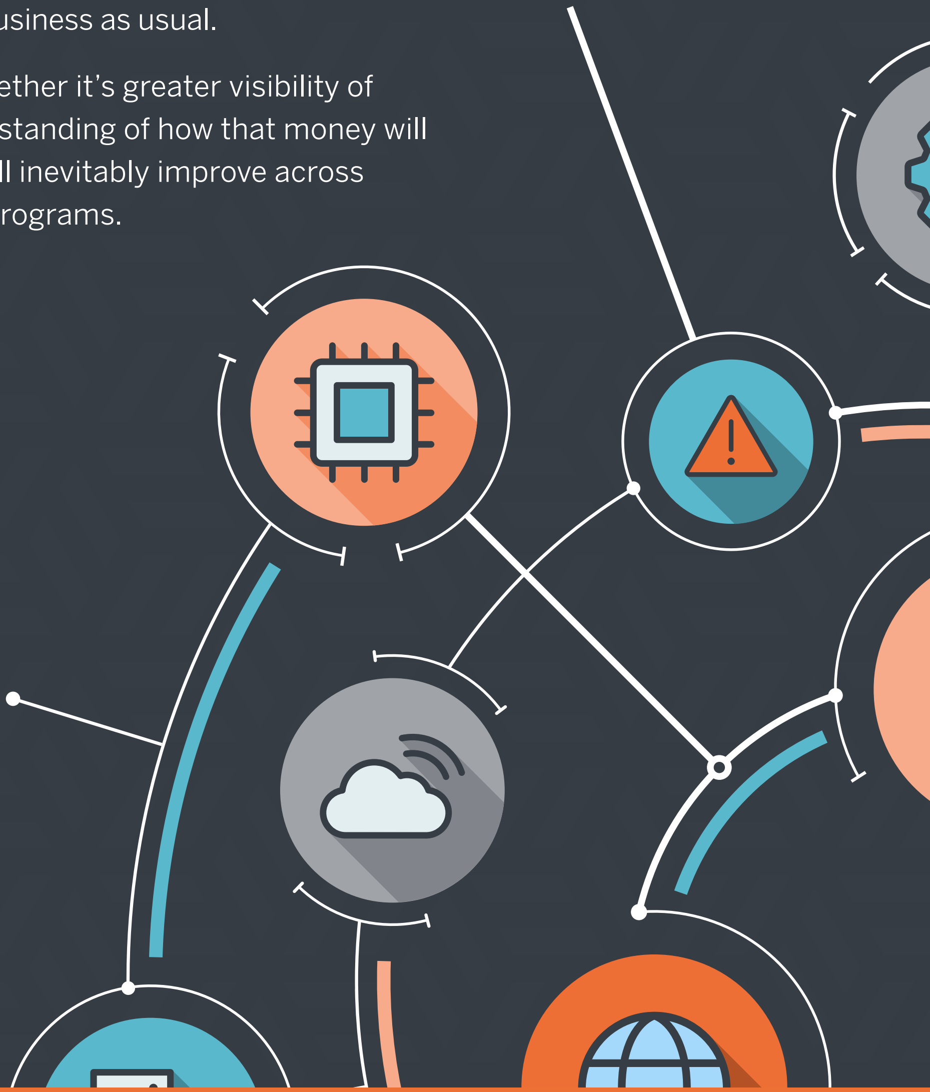
Improved cybersecurity is a key component of the federal government's effort to reduce risks to critical systems and sensitive data. These systems must be operational, secure and available 24/7.

Central to these efforts is the ability to understand what is being spent on cybersecurity today, what will be needed in the future, how that money is being allocated and whether those investments are sufficient and add value.

"But agencies won't know these things until they can get a very crisp, crystalized view of cybersecurity spending that aligns with the NIST Cybersecurity Framework and TBM," Carter said. These approaches help agencies to identify tradeoffs, make decisions on how best to maximize cybersecurity investments and protect applications, and ultimately carry out their missions.

For agencies that are in the early stages of this transformation, take the time to educate your staff on what TBM adoption will look like at your agency, and the benefits you anticipate. Ensure they understand how it pairs with the CSF and the potential risks that come with doing business as usual.

As agencies start to see quick wins — whether it's greater visibility of cybersecurity spending or a better understanding of how that money will be spent in the future — cybersecurity will inevitably improve across departments, sub-agencies, offices and programs.



About Apptio

Apptio is the CIO's business management system. We build advanced data and analytics applications that help all IT leaders understand and make informed decisions about their technology investments, capitalize on the cloud transformation and drive innovation within their organization. We call it Technology Business Management.

For more information, please visit www.Apptio.com.

About GovLoop

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 270,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

govloop.com | @govloop

govloop

govloop

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop