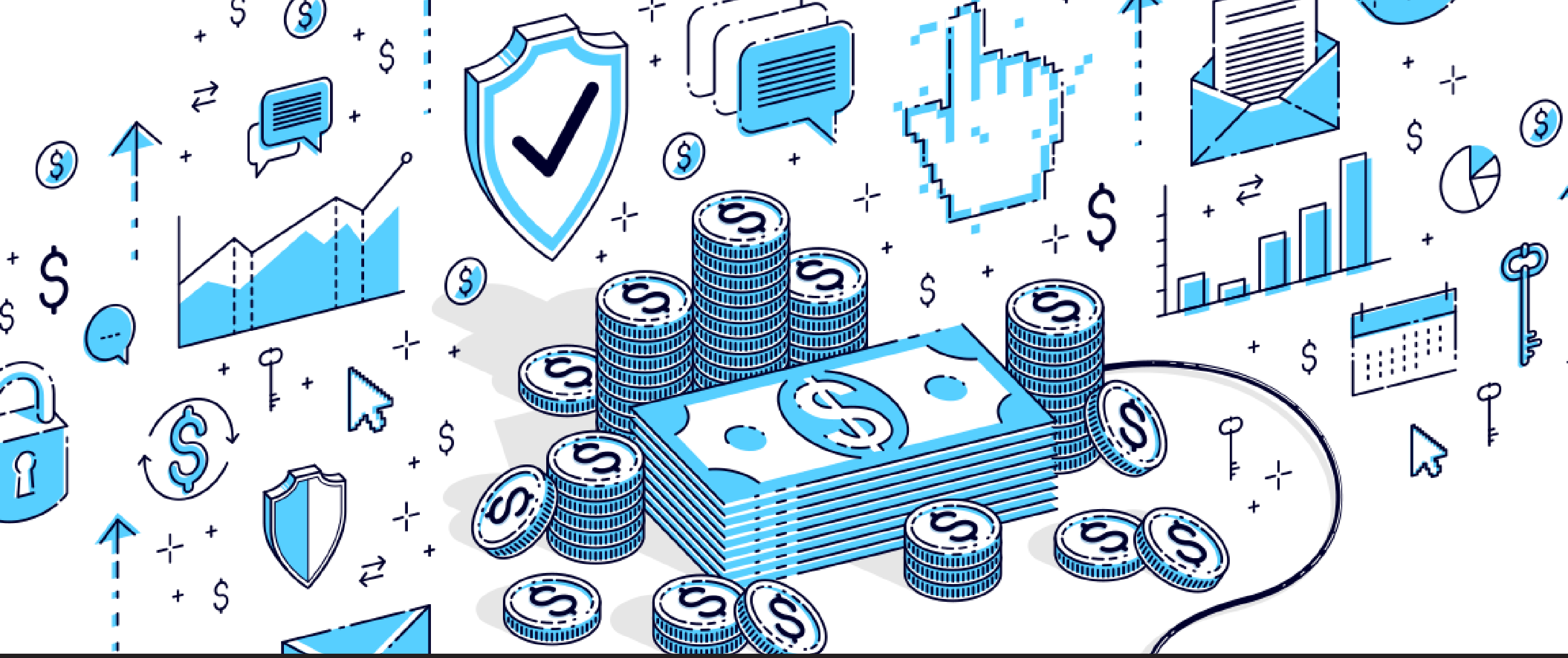

Five Steps to Building a Better Cyber Budget

Devolutions

THIS ARTICLE WRITTEN BY TIM MULLAHY, EXECUTIVE VICE PRESIDENT AND MANAGING DIRECTOR AT LIBERTY CENTER ONE, IS PART OF OUR GUEST BLOG SERIES.

PLEASE CONTACT US IF YOU WOULD LIKE TO BE FEATURED ON OUR BLOG.

There's a pretty good chance your business's cybersecurity budget needs some serious improvement. Don't feel too bad – you aren't alone in that. I'd honestly go so far as to say that the majority of businesses aren't budgeting IT effectively. Today, we're going to talk about how you can be in the minority that does.

Especially in smaller organizations, it can be somewhat difficult to put together an effective cyber budget. Where do you start ? How do you ensure you invest exclusively where it would be most effective ? How do you ensure you're not spending too much – or worse, not enough ?

Today, we're going to talk about that. I'd like to get one thing out of the way first, though. This won't be easy. Making sure your infrastructure and cybersecurity are up to snuff is an involved, comprehensive, and oft-challenging process.

It's also a necessary one.

Start at the Top

The traditional approach to IT, particularly where cybersecurity is concerned, is to evaluate on a case-by-case basis. If a new threat emerges or a new need arises, you analyze the situation and decide whether or not to invest in new systems. Eventually, those systems become part of an overarching strategy.

There's still place for a risk-based and needs-based approach in your budget. You should have some funds set aside for dealing with the unexpected. However, you should also take a step back to examine the bigger picture.

What I mean by that is that you must consider what your business needs. What are your specific priorities in terms of user enablement and workflows ? What specific goals do you hope to achieve with your IT spending ?

And from a security perspective, what assets do you need to protect, and why ?

The answers to these questions should form the cornerstone of your business's IT strategy. That strategy will inform the business processes you incorporate and the IT systems you adopt to support them. As already established, part of that strategy should be how your business will respond to unexpected risks – its crisis management and disaster recovery plans.

Speaking of risks...

Know Your Risk Profile

What assets and data are critical to your organization, and what steps have you taken to protect them from risk? When dealing with cybersecurity, that question is more important than any other. And the answer, as you might expect, has multiple facets to it.

First, consider where critical data is stored, how it is used, and who has access to it. Consider also what systems and processes are in place to protect it. If you don't like what you see – or worse, you have no idea what you're looking at – your first step is to dedicate time and resources towards improving your organization's data hygiene.

It may be both expensive and time-consuming, and it may require bringing in a third-party expert, but in the long run, it will be worth it, making any breaches you suffer simpler to mitigate and allowing your clients better peace of mind.

Beyond that, you need to consider who might want access to your systems and data, and why. Every organization is under threat from non-targeted attacks like ransomware and malware, so having something in place to mitigate those is a given. What you need to further consider is what threats and risks you face that are unique to your business and industry.

Evaluate Every Asset

Risk profile aside, it is also essential that you consider how each one of your business's cyber assets fit into your overall infrastructure – and your guiding strategy. An asset that's rarely used outside of a few fringe cases might not be worth continued investment, but an older system that's frequently required by staff across your organization could justifiably be upgraded. I'm not just talking about large, critical assets like servers and networking switches here either. I'm referring to more mundane stuff. Old printers and phones. Outdated desktops. Old smartphones and tablets. Anything else that might be aging and seeing less use – or simply collecting dust in storage.

Consider Using a Framework

One of the best recommendations I've seen where security spending is concerned is to use a framework like NIST or ISO27001 to assess your overall security posture. Doing so will help you determine what you're doing right – and where you're still weak in terms of your security approach. It's also advisable to bring in a third-party consultant or invest in an AI-driven solution to help you along if you have the funds for it.

Always Keep an Eye Out for ROI

It's a sad reality that most CIOs don't have full control over their IT budget. As such, every time you make a purchase – no matter how small – you should do so with a mind for how you can justify your return on investment. Not only will doing this consistently help you secure budget increases down the line, it can also help your executive board see the importance of the systems and processes you've put in place.

Again, this goes back around to the advice we've given on using frameworks like NIST, which provides metrics such as cyber strength. Other metrics could include hours saved, cost reduction, and revenue gained from new lines of business.

Above All, Communicate

At the end of the day, digital transformation and cybersecurity are not the responsibility of one employee or department. They're an end-goal that must be shared by everyone within your organization, from the most seasoned executive to the newest intern. With that in mind, I've saved the best advice for last.

Collaborate. Talk to staff about their needs, talk to your C-Suite about their goals, and talk to colleagues about their opinions. Involve everyone in the process of devising your budget, and ensure that everyone has a chance to share their thoughts.

In so doing, you'll not only ensure you're directing your attention properly – you'll also help your staff feel more engaged, interested, and, ultimately, satisfied.