expel™

Oct 16, 2017 | Bruce Potter

Budget planning: determining your security spend

It's a common question: "How much should I spend on cybersecurity?" Looking at your peers, analyst guidance, and postings on random security companies' websites, it's a difficult question. And there's not a one-size-fits-all answer.

It may seem counterintuitive, but how much you spend on security is really a trailing indicator of how your company views security. In corporate life, we're asked to set a budget long before we'll actually spend the money. So, we talk to our staff, we talk to company leadership and we attend conferences to figure out what we should be doing about cybersecurity and cyber risk management in our organization. Then we put together a budget, which gets kicked around for a while before it's eventually approved. A few months later we, start finally spending those budget dollars. But by that time we're really implementing our vision of security as it was 6 or even 12 months ago.

What bucket are you in?

What your vision is depends a lot on how your company views cybersecurity. I've found most organizations fall into one of five buckets. Do any of these sound familiar?

Security as an enabler ($$$$) – These are businesses that view cybersecurity as a differentiator to their service or product. They're implementing "leading edge" security solutions in an effort to set them apart from the pack.

Risk based ($$$) – Organizations that have risk-based cybersecurity are constantly making tradeoffs between required security controls and their risk appetite. While spending in these organizations can be high, it's also organized and controlled.

Security as a requirement ($$) – Some businesses use regulatory and industry requirements to guide their spend. This is often less expensive than a risk-based approach but it won't have the same coverage of controls.

Yet another piece of IT ($) – In these organizations, security is managed like IT spend, which for the most part means minimizing cost and not pulling from the bottom line.

Reactionary ($?*!$) – This is the "let the winds blow us where they may" strategy of cybersecurity. When things go badly, there's a large spend. When they go well, the spend is minimal.

Real Dollars

By now I'm guessing you've plotted what bucket your organization is in. But practically, how big are those dollar signs? According to Gartner, cybersecurity spend can vary from 1% to 13% of the overall IT budget. That's a pretty big range that doesn't speak well to the maturity of the state of the security profession. At the low end of that spend, you'll have organizations with minimal security controls and security incidents that go undetected and unaddressed for long periods of time. At the high end, you've got armies of dedicated staff, heavy tolling and engaged executives sponsoring cybersecurity initiatives.

Be aware, though, that absolute dollars are only one measurement. It's important to understand where this money is being spent… or more appropriately where it *could* be spent. Cybersecurity spend comes in many forms including staff, security software, hardware, contractor support, and outside services. Depending on your needs, you'll find you get different levels of value depending on which buckets you spend your dollars in. For instance, in a small organization that is sensitive to hiring more staff, contract support or outside services may be a better bet than ramping up staffing. In larger, more sophisticated organizations, spending on software and hardware that automates existing security controls and processes may be the best thing you can do. Each approach has a different price tag and will affect where you land on the one to 13 percent spectrum.

Find your focus (aka it's all about outcomes)

If you're struggling to figure out what type of security organization you're trying to be and what your long-term strategy is, my advice is to focus on your desired outcomes – both in proactive and reactive situations. Ask yourself: "What outcomes do I want, and when do they need to be possible?" Combine the answers to help focus your initial budget thinking… or at least rationalize your planned spend and set company expectations on realistic outcomes. If your budget and expectations don't match (typically the budget is too small to meet the desired expectations) you need to do one of three things: 1) get more budget, 2) right-size expectations, 3) find a new job proactively because this story won't end well and you will likely be the scapegoat.

Avoiding the trap door when you're in the breach zone

There will always be ebbs and flows when it comes to how much money there is to go around. Everyone has lived through a budget crunch at some point and had to tighten belts and live off less. On the flip side, if you've suffered a major security event recently, your budget likely got a bump to help you deal with the breach, response activities, and remediation. I call this the "breach zone". If you've been there you've probably also witnessed the "panic spending" that typically follows. Spending that windfall quickly is often seen as a proxy for progress. But it can also be a trap that sets you up for failure down the line. Why? Panic spending often results in buying products and services you don't ultimately get value from. What's worse is that you're then stuck paying for those products out into the future – increasing your long-term budget needs even more with things you don't need. Not to mention the time it takes to maintain them. It's a bit like stretching to afford a sports car but then you realize you can't afford the expensive gas and insurance.

A healthier approach is to use the specter of a breach to drive your budgeting process. If you're lucky enough to have escaped a breach, congrats. Pretend you have and go back to that outcome-based approach I talked about earlier. What do you need? What would you want to change in your org to achieve them? What investments would you make and what would you do differently? Use those answers to guide your budget process. Scenario based budget planning can help you build a budget for the security you're likely to need and

ensure your spend is on target with what your organization requires in the future.

Finding your spend

Based on all this, the question still stands: “How much should I spend on cybersecurity?” The answer to that question is unique to each organization. As I said at the start, there’s no one-size-fits-all answer. It depends on your maturity, current capabilities, executive support, and threat model; you may have wildly different spending needs than your peers.

But there are some things you can do to find the budget that’s right for you. Review your past spend and do an assessment. Did you get the results you want? What would you have done differently? Tabletop some terrible events like breaches and insider attacks. What would you need to respond? What would you need to stop it from happening? Use these answers to drive your budget and spending decisions. And remember that your budget is your own. Just because another organization is spending more or less doesn’t matter if you’re getting the results you want.

--

Visit the EXE blog for more articles like this at https://expel.io/blog