Security budget development using the “Charlie” method

Steve Hurst, CISSP, ISO 27001 Lead Auditor
Director, Security Strategy & Compliance
AT&T Technology Operations

A budget is like a roadmap and should be a critical component of your cybersecurity strategy. When planning a trip you have a starting point and a destination. Getting to your destination is your strategic vision. The mapped course is your strategy to get there. Now just like when you’re mapping a trip you may choose to take some side trips along the way, and may need to alter your course. So when developing your cybersecurity budget think of it as a way to realize your strategic vision. Working towards a long term goal will help you to see each year as a part of the journey and should help to make the budget process at least tolerable if not an enjoyable portion of the year’s activities.

Budgeting is not an exact science. The budget you develop and propose is rarely the budget you are given after it has been rolled into the overall budget and then parsed out. The method described herein reflects overall general principles, not a method specific to any given organization.   I once had a business manager who helped develop and keep our security budget on-track while meeting business requirements and continuing to maintain our strategic direction. To make this process work we used “the Charlie” method of budgeting. Most of you are probably wondering, “What is the Charlie method of budgeting?” Charlie is the oldest son of my former business manager who would help develop final budget numbers from the rough order of magnitude options developed based on our strategic direction and needs of the business. Before we get into the details of the “Charlie” method let’s look at the items we considered to develop those initial budget numbers.

Developing a budget to limit the cyber risk to an organization can be a stressful experience. Balancing maintenance with development adding in a dash of compliance or legal requirements and something to cover unforeseen expenses helps to establish your anticipated costs. Then there are unexpected expenses that could be the result of a technology change, a cyber-attack, or simply a change in the regulatory environment. In many organizations the IT Security budget is a part of the overall IT budget and therefore can be a place to save when budgets start to get tight.

Because the importance of IT or cybersecurity is so high I am of the belief that organizations should split their security budgets out from the oversight of the IT budget. By considering security as an operational expense, capital funding to maintain and upgrade security hardware that has been purchased becomes a business priority. This alone can help to reduce your risks as you have budget to replace solutions that are getting ready to go end of support before they stop getting patches and become risk generators.

Speaking of risk, regardless of where the budget is controlled from, you need to consider where to use your money to maximize its value. There are a couple of items that can be done to significantly reduce your risks. Starting the evaluation process with a security or risk assessment is a good way to start your budget process. Assessments help to show you where vulnerabilities are and the level of risk these vulnerabilities add to the organization. You can then plan to spend more money in the areas that will reduce your risk the most. Some of the areas found to help reduce risks quickly and affordably include: user education, keeping an accurate inventory, patching quickly, replacing end of support hardware, secure remote access, and having an up to date cyber response plan. These activities should be included in your cybersecurity budget and will also help you to measure your effectiveness (which can become one of your measurement criteria to show benefit).

The next step in the budget preparation process is to look at your expenses over the past few years to set an expense baseline. Are there things that you wanted or needed but couldn't invest in? What worked well and what things could be improved upon? Are there upgrades that were delayed? These are some of the questions to ask yourself when setting your risk baseline, the risk baseline defines what budget amount it will take to maintain the organization's current level of risk. When evaluating your previous year's expenses, I suspect you will find that staffing is the highest expense line in your budget. This leads to another key budget question, "Should you insource or outsource security operations?" The answer to this question is not an either/or response as you can combine the two options and, in my opinion, should always keep the ultimate responsibility for cybersecurity policy in house. The answer on where to source the work can make a significant difference in your "Rough order of Magnitude" budget numbers. While I'm not going to recommend a specific solution, the keys are risk reduction, operational simplicity, and staffing.

Solution design reviews would be my next step in the budget process. Does the current solution reduce your risks to an acceptable level? Is this architecture as simple as it can be and still maintain its effectiveness? Basic engineering principles tell us that complex designs have a higher chance of breaking, or in this case increasing the number of possible cyber security vulnerabilities. When evaluating or designing a cybersecurity solution I recommend looking at the KISS principle or "Keep It Simple Stupid." By designing to as simple a solution as will be effective you help limit your risks and costs. Part of this evaluation will include looking at new technologies that could help to reduce formally unknown risks or finding ways to simplify the architecture you currently have in place. When looking at technology it is important not to be too technology focused. Look at the results, compare the results to the vulnerabilities you need to care for. Be creative, look at alternatives and expand your options into the realm of what should be possible not just who came into your office last. With more security, and networks, moving into the cloud or being truly software based there are options available you may not have thought about in the past. These options may be able to help you both reduce costs and risk.

Having looked at risk, design, and technology, generally the single largest portion of your budget will be staffing. Today, the effective employment rate for cybersecurity experts is in the negative numbers as there are more employment opportunities than there are candidates to fill them. Because of this unusual employment situation, and the time it takes to find candidates for open positions, budget money should be planned for to help with employee retention. According to "TalentSmart" (http://www.talentsmart.com/articles/9-Things-That-Make-Good-Employees-Quit-172420765-p-1.html) the top reasons good employees leave can be summarized into a few categories: overworking your staff, under recognizing your staffs contribution, a lack of honesty or keeping your promises, not using the creativity and passion of your staff, and failing to develop people skills. This, and other research, shows that pay is not the reason people leave their current employers. To help curb this situation, make sure you budget includes funds for staff development, skills training, travel related to training, and employee recognition.

The flip side of employee retention is employee reductions as an organization strives to be more cost efficient. Plan and budget for increased automation and the benefits that come from automating repetitive tasks which should be lower costs or provide greater productivity. As machine learning and

Artificial Intelligence (AI) continue to develop you can start to plan for staff reductions when balanced with the appropriate automation or outsourcing. Given the demand for security expertise and the desire to control costs budgeting for automation projects will help justify the retention of top talent and a reduction of costs over time. When adjusting staffing, it is important to pay attention to what is known as “the bus” scenario, where your expertise is limited to one person and you lose those critical abilities if they leave or get hit by a bus. As with any other critical system, budgeting for staff redundancy can be critical for ongoing operations and creates a good reason to cross train your staff.

Now we are back to setting rough magnitude budget numbers before we make use of “the Charlie” method. Let’s look at the items that need to go into our budget number:

1. The cost of a risk assessment to assess where there are gaps in the current security solution. This activity is not only helpful but may be required by third parties, like the Payment Card Industry (PCI) to process credit cards or may be required by law
2. What is the existing operational security spend (what it will cost to “keep the lights on” and continue to operate the infrastructure currently deployed)? Is this number trending up or down?
3. Are there projects that need to be developed and implemented to keep risks at an acceptable level? What are the estimates for those projects? I suggest having them prioritized so you know what can be delayed based on the budget negotiation process.
4. What level of spend can you justify for new technology? If you spend some today can you save more tomorrow? Have there been legislative initiatives put in place, or expected on the docket, that will require new or upgraded solutions to be deployed?
5. Staffing, always a hot item, will it go up or down? Assuming down, by how much? Does this make outsourcing more or less attractive? If staffing goes up, how much of an increase will be approved and when will you plan on bringing the new team members onboard? How will the cost of automation projects impact the budget and will they result in cost savings or productivity increases for the next budget year?
6. Staff retention. It is always less expensive to retain good staff then to replace them. Look at what it will take to keep your team interested and excited and add that to the number.
7. Now for the fudge factor. Every year there can be unexpected activities that can drive up spending. With the explosion of ransomware make sure there is money budgeted to restore data from a backup instead of paying a ransom, which historically may not work or may lead to additional ransom requests. This, and other unexpected events, would go into the fudge factor of your budget.

When you add these items together you will come up with a budget number that, will most likely be unrealistic. Write this number down on a piece of paper. Now walk through, preferably with your team leaders, different things you can eliminate to lower your proposed budget number. Write these down too. When documenting the budget options make sure you have a record of the calculations to get each option.

Now we come back to the “Charlie” method. We would take the budget options that were developed and put each on a piece of paper and crumple them up. Now Charlie loved to chew on paper so we would scatter the different budget options now crumbled up pieces of paper around him and wait. As small children will do he would start to play with the paper and eventually put one of them into his mouth. Being a new mother, my business manager would then take the paper away from him and present Charlie with a small cookie. The number chosen by Charlie would be submitted with the appropriate business case. As is typical in most organizations a different number than the one submitted would come out of the budgeting process. We would then focus on managing to the budget number we were given.

During the time Charlie was young enough not to have an opinion, or complain too loudly, we managed to get that budget number approved and be within 10% of our budget number every year. Why 10%? You'll have to read the upcoming blog on security budget management.