An Executive's Guide: How to Align Your Cybersecurity Spending With Risk Tolerance

TBCONSULTING

Introduction

For most businesses, cybersecurity makes up only 10% of the overall IT budget. Is that enough or too much? The answer is unique to your organization, but relegating cybersecurity to a line item in the IT budget is a risky proposition. Underinvesting in cybersecurity can adversely affect the business outcomes of an organization. Overinvesting in cybersecurity tools without achieving measurable protection is a waste of resources.

Cybersecurity initiatives are often difficult to budget due to misalignment of goals and expectations between executives and IT leadership. While CEOs are responsible for formulating a business strategy that invests in outcome-driven goals to drive profitability for stakeholders, IT leaders ensure that the company's technological resources operate at peak levels while mitigating risk.

So how can the CEO and IT leaders sync up to enable the organization to achieve profit-driven performance? They can start by utilizing a cybersecurity framework to determine the resources they are willing to invest, balanced against their acceptable risk profile and desired business outcomes.

"In 2021, 55% of enterprise executives plan to increase their cybersecurity budgets and 51% are adding full-time cyber staff."

- Forbes, December 2020

Maybe you have the best security tools and have made significant capital investments, but you still don't feel that you are getting the value out of your cybersecurity spend? Increased spending and additional tools do not necessarily add up to better protection. Executives and IT leaders need to balance expenditures with coverage - after a thorough evaluation of the unique risk factors of their business. In this way, leadership can determine that the spend is worth the benefits in risk reduction and that critical business operations are prioritized.

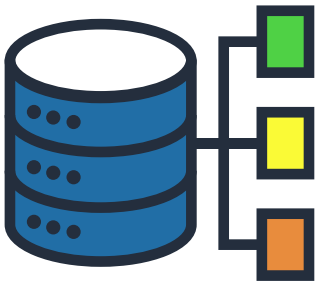
Have you implemented a security strategy based on a cybersecurity framework? To build a robust security strategy, leadership teams must collaborate to find and utilize a cybersecurity framework that works for their business. In this way, the company can create a plan and a budget to reduce cyber risk and support growth.

Sounds simple, right? Then why do so few executives take the time to develop a security strategy that is aligned with their organizational goals? Why don't they utilize a cybersecurity matrix to identify where to prioritize the protection of their most valuable data and business-critical workflows? It could be that they lack the experience to implement a cybersecurity framework and do not understand how to measure cybersecurity maturity against the company's risk tolerance. Risk mitigation is an organizational challenge – executives must communicate the needs of the business and align those with IT capacity, thus accepting "x" amount of risk at "y" cost.

Executives understand the danger cyberattacks and ransomware pose to their business, and often react to the threats by overspending on security tools to protect themselves. An experienced Managed Security Service Provider (MSSP) can help your company determine the right budget for your cybersecurity maturity profile with adequately funded investments in people, processes, and technology.

3 tips to make sure your cybersecurity budget is right-sized

Utilize a NIST Cybersecurity Framework to map risk against budget



Maximize your cybersecurity tools with proper integration

Strategize with the cybersecurity experts

Tip #1: Utilize a NIST Cybersecurity Framework to map risk against budget

- **Why do you need a standardized cybersecurity framework?**

How valuable are reliable operations and secure service delivery to your organization? Not the type of service delay caused by internet latency, but rather when malware hits your unmonitored network and your business grinds to a halt. Your employees cannot work, your customers cannot contact you to conduct business, and company data is on the black market. If you cannot engage in business, you are not in business.

Modern business outcomes are often based on technological capabilities. In order to maintain, and have the ability to restore operations, the relationship between business and tech needs the support of a prescriptive cybersecurity framework.

To verify the success of your cybersecurity program, you need metrics around your current state of cyber maturity. How do you measure success when a decrease determines success? There is no doubt that your business will profit from decreased risk. But it is impossible to determine your company's level of cybersecurity coverage without a foundational framework. You can also use that same cybersecurity framework to map out controls and governance to be implemented across your environment to improve your maturity profile.

- **Start with the NIST cybersecurity framework**

The U.S. government offers organizations a simple, standardized security framework known as the National Institute of Standards and Technology (NIST) cybersecurity framework. NIST offers core standards to measure your cyber risk against the business outcomes you can expect to achieve.

For a visual reference of the following information, the Federal Trade Commission offers a great infographic on "Understanding the NIST Cybersecurity framework" here.

Based on the following NIST pillars, organizations can tie operations and service delivery to an appropriately funded level of acceptable risk. Unless your company has a bottomless budget, you will not reach 100% security coverage; thus, you need to determine how much risk you are willing to accept.

- **Identify**
  Identify the threat landscape with tools like vulnerability scanning, network mapping, and domain auditing. Identify every single asset running in your environment.

- **Protect**
  Implement end-user security access management with multi-factor authentications. Employ educational training for employees to actively monitor email accounts to detect phishing emails, and to avoid opening dangerous attachments.

- **Detect**
  Integrate your security incident event management (SIEM) and network intrusion detection system with an endpoint detection and response automation framework that is then tied to your network and firewall.

- **Respond**
  Use an automation framework to contextualize reports, prioritize alerts, triage incidents, produce ticket assignments, and run playbooks on a single collaborative framework.

- **Recover**
  Measure restoration capabilities by the time it takes to return to standard business functionality after an impacting event. It is essential to analyze data from each recovery in order to update process plans. Determine your backup and restoration capacity (how fast you need to be up & running after an incident).

"We are seeing a rapid evolution and increase in cyberattacks targeted at the large expanded digital footprint that organizations are amassing today. The pandemic has reinforced the critical need for cybersecurity programs that are agile enough to react to minor and major extraneous shocks."

- Gartner, April 2021

- **Build your cybersecurity strategy based on a security framework**

It is costly and exhausting for IT teams to remain productive in a reactionary cycle of fighting fires. But when organizations proactively build strategic processes around data security, they can position themselves to lessen the impact of cyber incidents. A security strategy that maps out business priorities and identifies critical data and workflows on the cybersecurity framework will support continuous business operations and service delivery.

The success – or failure – of your current security posture may be measured against the cybersecurity framework. These metrics allow executives to make outcome-driven decisions about future security investments. If executives can accurately determine their risk tolerance, they can justify security investments for the appropriate amount of coverage.

When organizations proactively build strategic processes around data security, they can position themselves to lessen the impact of cyber incidents.

But how much coverage do you need? It depends on the priorities of your organization and the maturity of your security posture. As you build your strategy, make sure to identify every asset, system, application, and network that could be a liability to your organization's security.

So now that you understand the need to implement a cybersecurity framework, how much should you budget for security coverage? Determine how much you are willing to invest in employee cybersecurity training, process enforcement, tools, and continued education for IT teams. Balance that against the cost impacts of a single security incident or an employee opening a malicious phishing email and infecting your network. The budgeting process is challenging, but knowing your cybersecurity maturity position can help inform the budget.

- **Determine your cybersecurity maturity based on the matrix**

The cybersecurity matrix measures your current risk profile across the 5 NIST pillars (Identify. Protect. Detect. Respond. Recover.). The matrix will help reveal gaps in protection and provide awareness around how you use your existing technology stack. It will highlight vulnerabilities and reveal the cybersecurity health of your organization. Ultimately, your cybersecurity maturity 'grade' will be based on how well you assess, monitor, and mitigate risk across your enterprise.

Once you have that foundational information, you can determine the appropriate level of risk that your organization is willing to accept; and then build an outcome-driven roadmap to meet your cybersecurity goals. And in planning for your future state, you can move across the matrix and incorporate additional protections, until your organization achieves your targeted cybersecurity performance.

Executives and IT leaders should collaborate to identify the benefits of tighter security controls and how IT investments will promote business outcomes, drive value, and contribute to revenue. Then determine how much you are willing to invest to positively impact your bottom line.

Ask questions like: Do we have the correct number of tools? Do we have the people, processes, and technology needed to meet our cybersecurity goals? Do we need additional guidance? Can we benefit from outsourcing cybersecurity monitoring to mature more efficiently?

It is far easier to defend the IT budget 'ask' and prioritize investments when you can see exactly where you stand and have prepared a roadmap to address your security strategy. Building cyber maturity is a process; no one tool will instantly provide total coverage.

"The siloed nature of today's security disciplines is quickly becoming a liability."

- Gartner 2021

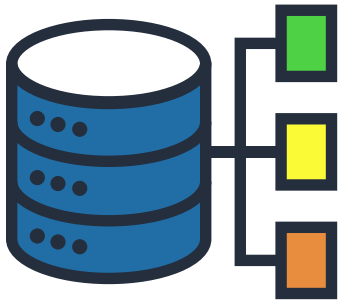
- **Build a tool and service-based solutions roadmap to maximize your coverage and reduce risk**

Build a solutions roadmap that addresses the protection of your devices, applications, networks, data, and users. Then employ a cost/benefit analysis to determine the appropriate level of risk that is tolerable for your organization and map top-tier protection tools to your most significant revenue generators, business-critical data, and operations. But do not rely on tools alone. Tools without integration are just expensive toys. Instead, invest in the people and the processes that complement the technology being implemented.

Cybersecurity budgets should remain flexible enough to cover organizational changes and priority modifications. In the mapping process, be sure to tie all the investments back to the support and protection of business outcomes and goals.

The ideal roadmap will guide the organization to understand the cybersecurity challenges they face and the level of risk they are willing to accept. If you track your budget and capabilities against your strategic roadmap, there will be clear metrics to measure success or failure.

Explore how tools are used, how assets are managed, how patches are deployed, and how threats are mitigated. Then, you will be able to adapt all those processes to increase protection. A tailored solutions roadmap can reduce costs associated with downtime, verify data backups with regular testing, and improve your cyber maturity score. Executive oversight ensures that the cybersecurity strategy is communicated to all employees, adhered to on a companywide basis, and reviewed annually to adapt to changes in your business environment.



Tip #2: Maximize your cybersecurity tools with proper integration

Your business may have purchased top industry tools for data protection, but if you're like 69% of organizations, you don't think your antivirus software is enough protection. So how do you know if you are getting the most value out of the tools your business already owns?

If you're like 69% of organizations, you don't think your antivirus software is enough protection.

If your IT team is in constant chaos despite every department being "tooled up," the tools are probably siloed with no standard methodology in place to address threats. Without integrated tools, there is no way to measure the effectiveness of the tools, there is no method to justify additional budget for cybersecurity. Only by integrating the people, process, and technology aspects of cybersecurity, can you expect measurable security protection and understand how each tool contributes to your overall cyber defense strategy.

LET'S TAKE A LOOK AT SOME OF THE COMMON PITFALLS OF HAVING TOO MANY CYBERSECURITY TOOLS

• **Limited protection** Tools are divided by team/department and may not focus on integration to inform company-wide protection. Without communication and info-sharing between business units, resources are wasted, and time-sensitive security data is not delivered to the people who can best provide solutions.

• **Siloed protection** You may have the most expensive and industry-leading tech tools available, but you have no way to measure the performance, coverage, or capabilities of each tool. You must tie the tools to the people and process components of the cybersecurity matrix. Tools should contribute to the overall health of the business, but they cannot provide value alone.

• **Checkbox protection** Your organization may need to beef up your tech stack to meet compliance requirements. But, even if you can 'check the box' that you have the tools, are they delivering true security benefits and data protection?

As cyberattacks are increasing in number and becoming more sophisticated, you need to take steps to strengthen your cybersecurity posture. Protect your business with a cybersecurity strategy that will help minimize your risk and inform your recovery processes for post-incident mitigation. When evaluating your current toolset and budget, find proof of the value of each tool or remove that line item from your budget.

Proof of value ensures that each tool provides meaningful metrics to the people in charge of implementing solutions and that those solutions align with your overall business strategy. Do you have vulnerability scanning but not an automation process to base threats on priority and impact to reduce risk? Do you have a backup solution, but have never tested it? Does your IT team have alert fatigue from tools setting off alarms from unverified threats?

Cybersecurity is not about buying the most tools. Cybersecurity is about implementing the best tools to optimize the collaboration, communication, capabilities, and protection for your organization's unique needs.

Tip #3: Strategize with the cybersecurity experts

Does your Board of Directors want to cut your IT funding? Or is IT leadership trying to increase the cybersecurity budget?

Suppose your current IT spend and coverage are not based on clear metrics. In that case, the budget is arbitrary and indefensible and can not pinpoint any quantifiable value for the business. Not surprisingly, executive leadership will require justification for any increases in IT funding as they are focused on ROI. Additional cybersecurity spending must add demonstrable value to the business.

But, if the budget for the cybersecurity strategy is not based on a standardized framework, the 'ask' for increased spending may be perceived as unjustified. It may be time to bring in outside security experts from a trusted Managed Security Service Provider (MSSP) to evaluate your organization's position on the cybersecurity matrix. An experienced MSSP can help you build a roadmap designed to align your cybersecurity program with your acceptable risk profile. Armed with this roadmap, IT leaders will be able to present quantifiable, business-specific metrics to the executive leadership team.

Since executive decision-making hinges on the combined consideration of risk management, exposure, and value, IT leadership must strive to align IT goals with overall business goals. Stakeholders want to know that the company is protected, compliant with cybersecurity regulations, and can expand IT capabilities to match the company's future growth.

Without a cybersecurity strategy, many companies react to increased cyber threats by overspending on tools to protect the business. But, when you can map your company's position on the cybersecurity matrix, your existing tool suite may be optimized by integrating the right people and processes to fill gaps in security. You may be able to reduce risk, decrease your exposure, and spend less when you invest in smart tools that can integrate across business teams. An MSSP will work with your business and IT leadership to tailor your cybersecurity coverage and determine an appropriate IT budget based on your acceptable risk level.

By outsourcing security monitoring to an MSSP, you will gain control and visibility of your environment through a single pane of glass. The result is that there are no silos, no disparate tools, no confusion about viable threats, and you avoid the alert fatigue plaguing many IT teams. The security protection delivered is based on your specific risk profile and budget.

MSSPs can make sure you are getting the value from your tools and optimizing your infrastructure's security performance. With ongoing cybersecurity monitoring and risk evaluation, an MSSP can increase IT awareness with meaningful security metrics while supporting and protecting your critical data and foundational infrastructure.

Conclusion

CEOs are accountable to stakeholders to drive value-based investments and outcome-driven profitability. Those business outcomes rely on implementing a clear cybersecurity strategy framed by a matrix to deliver comprehensive risk mitigation across the business environment.

Cybersecurity is a critical element of business success. All stakeholders (executives and customers alike) feel the impact of a significant cybersecurity attack. To remain profitable, and able to quickly address threats and remediation efforts, you need to rely on a cybersecurity framework. Executives can then architect a defensible security strategy based on metrics to inform IT budget decisions. Executives need to work collaboratively with IT to balance risk with the IT budget to optimize the value of cybersecurity.

Unless you already have dedicated security practitioners, a fully staffed security operations center (SOC), a security architect, and senior engineers in-house, it makes good business sense to rely on an MSSP to support your IT management. Security experts at an MSSP understand security strategy and profile evaluations and can implement comprehensive coverage based on your risk profile.

TBConsulting is an MSSP with 25 years of IT experience. Our security experts are dedicated to building cybersecurity strategies that address the unique needs of our clients. TBC can help design a security strategy for your organization and provide continuous security monitoring, so you are able to focus on business outcomes.
IT budget to optimize the value of cybersecurity.
Unless you already have dedicated security practitioners, a fully staffed security operations center (SOC), a security

Click Here for a Quiz to Evaluate your Cybersecurity Maturity