BRIDGING THE GAP

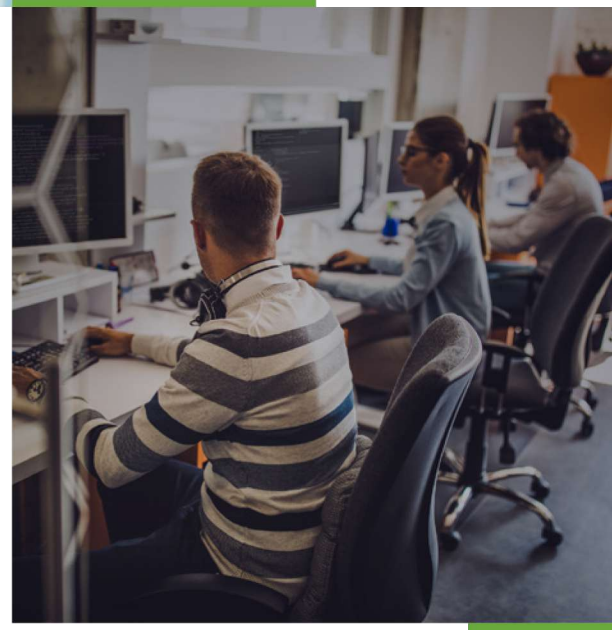
How to Win the Cybersecurity Skills Shortage

GreyCastle security

TABLE OF CONTENTS

INTRODUCTION

There seems to be no end in sight for the cybersecurity skills shortage—and it seems to be getting worse rather than better. Nearly three quarters (74 percent) of organizations report they have been impacted by the shortage, according to a global study of cybersecurity professionals conducted by the Information Systems Security Association (ISSA) and Enterprise Strategy Group (ESG). The report also concluded that the skills shortage has contributed to the rise in security incidents, as organizations lack both the required end-user awareness training and the necessary amount of staff to keep up with increasing cybersecurity workloads.



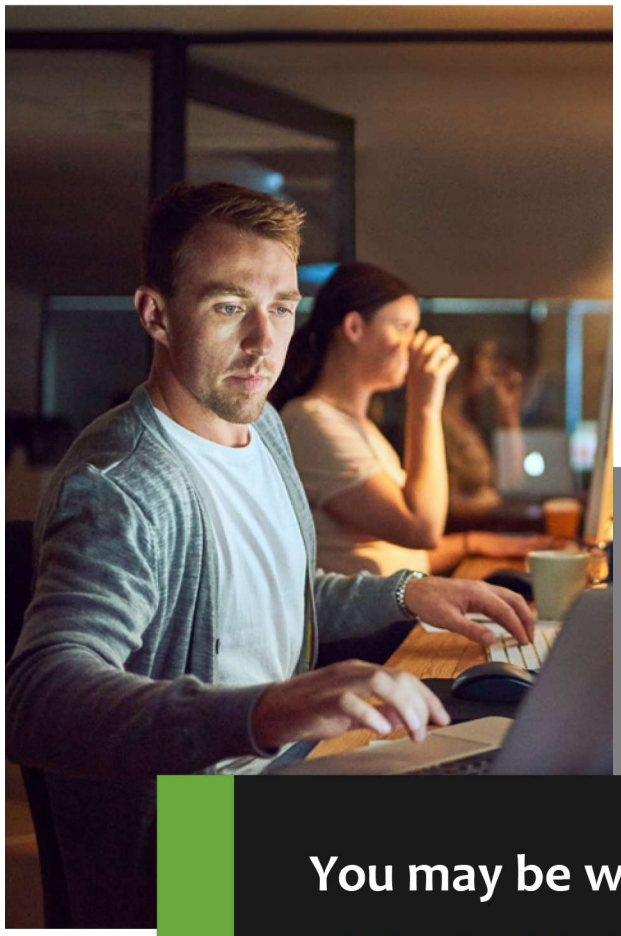
Think of it this way:

What's the good of having a fleet of brand-new firetrucks and top-of-the-line hoses if you don't have firefighters nor a procedure for putting fires out?

Over the past decade, the demand for cybersecurity solutions has far outstripped the supply, causing organizations to struggle to make real progress. People spend a lot of time talking about technical controls, firewalls, and risk management, but at what point do we stop talking and start doing? **This is where the cybersecurity skills shortage presents a problem.**

Your customers and clients expect you to keep their data safe. When you lose their trust, you'll face financial consequences. Companies that lost less than 1 percent of customers after a data breach experienced an average total cost of $2.8 million, according to the "2018 Cost of a Data Breach Study" conducted by the Ponemon Institute. If the organization lost 4 percent or more of customers, the average total cost was $6 million. The cybersecurity skills shortage can have a powerful impact on your bottom line.

With the cybersecurity workforce gap reaching close to three million globally, according to the (ISC)² Cybersecurity Workforce Study, it's becoming more difficult for organizations to protect their own assets and secure client data.



You may be wondering:

Why is this happening and is there anything my organization can do to combat it?

THE PROBLEM FACING CYBERSECURITY

The cybersecurity skills shortage poses a threat to all organizations and has the potential to cripple the growth of businesses across all industries. The fact is, the current approach to solving complex cybersecurity problems and the associated staffing issues aren't working. **Here are some reasons why.**

Success Requires Expertise

The intensity and scrutiny on cybersecurity standards has increased many-fold over the past five years. Organizations have either known of, or been practicing, established cybersecurity standards (e.g., NIST SP 800-53 or ISO 27001) for many years. What has changed is the breadth and depth of cybersecurity as a practice. The kinds of things that information security professionals are being asked to do today (whether by a third-party, customer, or the federal government) have become so vast that the cybersecurity team of yesterday wouldn't be able to accomplish them.

For example, within the NIST Cybersecurity Framework, there are upwards of twenty different cybersecurity domains. Each of these requires its own expertise and experience; includes its own challenges; and has established solutions that you may or may not be aware of. That's just one example of how big this thing called "cybersecurity" is. What information security teams are being asked to do has expanded significantly. If you want true experts —those with experience and skills working in access controls, incident response, policy development, governance, compliance, and so forth—**it would require approximately five to fifteen individuals with completely different backgrounds, experience, and certifications.** This becomes a massive undertaking and introduces new challenges into the organization.

Resources Are in Short Supply

We're still in the beginning stages of cybersecurity as an industry, and so, the manufacturing of talent hasn't yet spun up. And this doesn't just apply to higher education's role in creating new talent. Approximately 63 percent of ISSA members reported feeling that their employer didn't provide the right level of training for cybersecurity employees. A related problem: 66 percent of ISSA members said that the demands of their job prevent them from developing critical skills. This creates a scenario in which organizations are both unable to source new talent and unable to bolster their current employees' skill sets. Ultimately, this hinders an organization's ability to mitigate risk and defend against cyberattacks.

Cybersecurity Ventures estimates that there will be **3.5 million open cybersecurity positions by 2021,** so this isn't just a "today" problem. There will continue to be a tremendous shortage of professionals who can perform the tasks that organizations will need them to do.

Resources Are Expensive

Anyone who has attempted to build a cybersecurity team can tell you two things. One, these professionals are expensive to hire. Two, they're only getting more expensive. This will continue to be a trend until supply has met demand and there's equilibrium in the market. Currently, the average salary for cybersecurity professionals is $116,000. That's almost three times the national average, according to the Bureau of Labor Statistics. A team of five to ten experts with the right skills and experience is really going to add up. And, if you also need to hire a CISO to lead them, Salary.com reports that the average salary for a CISO in the United States is almost $223,000.

Resources Are in High Demand

In (ISC)²'s 2018 "Hiring and Retaining Top Cybersecurity Talent" report, 70 percent of cybersecurity professionals surveyed said they'd be willing to move to a new opportunity if approached by a recruiter—even if they previously had no plans to begin a job search. So, experienced professionals are not only difficult to find and expensive to hire, but they're also difficult to retain. This often leads to organizations competing against each other to offer higher salaries, better benefits, and unique perks. This might be easy for Fortune 500 companies to offer, but what about smaller enterprises?

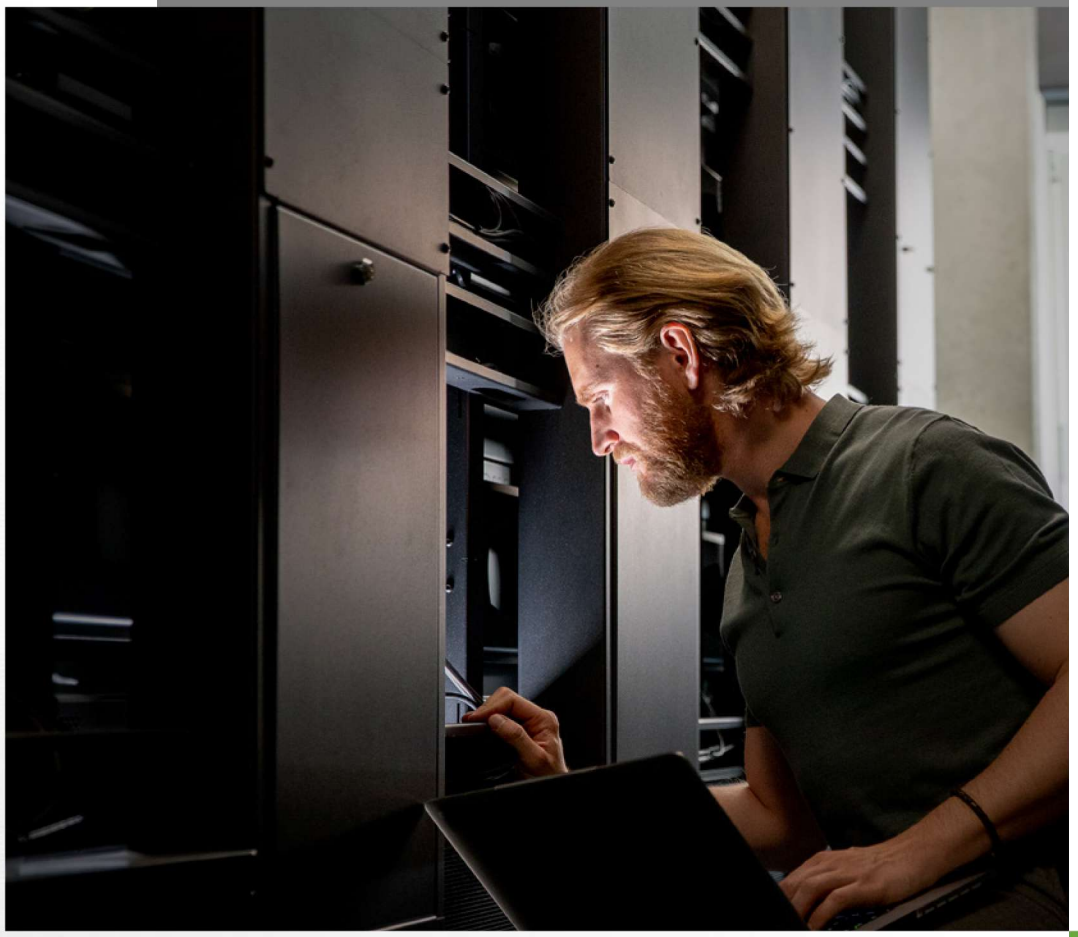
Your experts are being hunted by recruiters and by your competition. While your organization may be facing regulatory pressures or malicious attackers, underneath it all is a foundation that honestly hasn't even been built yet. The resources organizations need to address these issues don't yet exist.

ADDRESSING CYBERSECURITY IN A MEANINGFUL WAY

Cybersecurity skills and expertise are increasingly in demand, all while supplies of these resources continue to fall flat. The reality is, the average business cannot practically build their own cybersecurity team.

But there's hope.

Organizations can weather the storm of the cybersecurity skills shortage by building a proactive program and partnering with experts to help them bridge the gap between the strategic use of cybersecurity and the enablement of business growth.



WHY (AND HOW TO) BUILD A PROACTIVE CYBERSECURITY PROGRAM

Cybersecurity is a strategic issue that often doesn't have the visibility necessary for the business to make relevant, practical, and effective decisions. This leads to several negative impacts, including a lack of accountability for risk owners; not having a defensible position; an inability to quantify the strategic importance of cybersecurity; and a failure to budget for cybersecurity at a strategic level. It can also create a false sense of security where technical solutions are seen as both the only option and the right option.

The complexity of today's business environment paired with advances in technology and the desire for a quick fix has left many organizations severely lacking when it comes to the basics of cybersecurity. **The primary focus of any cybersecurity program should be knowing what our risks are and what we should be doing about them.** With that in mind, how can organizations ensure they have a method and a means to communicate these ideas across the business?

First, everyone needs to be on the same page. The vision for cybersecurity within a business needs to reach everyone from the board of directors to the junior network administrators. Thankfully, there are defined processes that organizations can leverage to guide this.

At GreyCastle Security, we recommend organizations follow six core steps for building a proactive cybersecurity program. Keep reading for a high-level overview of these steps.

01 Identify and Inventory Data Assets

Build a comprehensive list of data assets. (Note: Data assets aren't the same as information assets. Information assets are things like servers, workstations, firewalls, and laptops that exist solely to process, store, or transmit data.) Data sets should be organized by owner and classification. In most cases, data is needed to run the business—and thus has an inherent risk. To build an inventory, at the simplest level, you'll need to interview each department and document what data sets they have, identify the volume of data, and identify the data owner.

02 Conduct a Risk Assessment

Once you know what your data is, how much you have, and what its value is to your organization, you can begin to talk about risk. The process of risk assessment enables a repeatable and measurable way for all parties to understand business impacts and select reasonable controls to facilitate remediation without having to understand the underlying complexities. Select appropriate standards for baseline/compliance and ensure the scope is clear and understood by all.

A key point to remember for the management of risk is to resist the idea of low-hanging fruit. If something doesn't impact your risk profile or reduce your risk in a meaningful way, don't do it.

03 Implement Governance

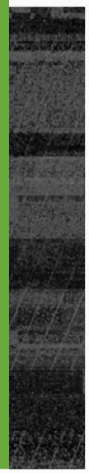
Governance allows you to effectively manage cyber risk in concert with your business objectives. Cybersecurity governance allows the organization to make strategic decisions, establish an appropriate level of security for the environment, inform the cybersecurity budget planning process, satisfy regulatory and legal requirements, establish ownership and visibility around risk management, and promot the clear communication of cybersecurity risks to senior leadership. An Information Security Officer may be appointed to lead governance efforts and ensure there's a high level of accountability. Governance is not a one-person job; you can't establish this function without including the right people and the right business units.

04 Implement Policies, Standards, and Controls

Participation and accountability is required from departments and individuals across the business. Cybersecurity is a strategic business issue and requires the involvement of strategic business leaders. Different business units will have ownership in multiple control families. Policies and standards need to be put in place to ensure each unit understands specifically what they own and what that means.

There are three to four major policy documents that an organization should have, including information security policy, data classification policy, acceptable use policy, and a privacy policy. It's recommended to have a single information security policy for all security efforts; don't create standalone policy documents. One policy for common functions reduces confusion and overhead, and enables compliance.

Policy sets the direction. The way to know if you have an effective policy is to ask yourself: Can somebody on the board (or equivalent) read our information security policy and comprehend it, understand it, and agree to it?



05 Implement and Align Cybersecurity Plans and Procedures

Plans and procedures should be developed using the policies and standards as key inputs. Your plans should address specific processes that require a comprehensive approach to be successful. Typically, plans are needed when multiple business units are required to build and execute, such as for incident response plans or business continuity plans. Process experts may be required to ensure the complex nature of these processes are appropriately implemented.

Procedures describe the "who" and "how" for implementing standards. They must be developed to ensure appropriate and repeatable processes exist to support the operational execution of security controls and standards. Procedures must use the clear guidance provided by the standards to be effective and in-line with business risk appetite. As plans and procedures are developed, gaps should be formally identified and sent to the governance team for resolution. Procedures are specific to the organization; think of them as your "secret sauce."

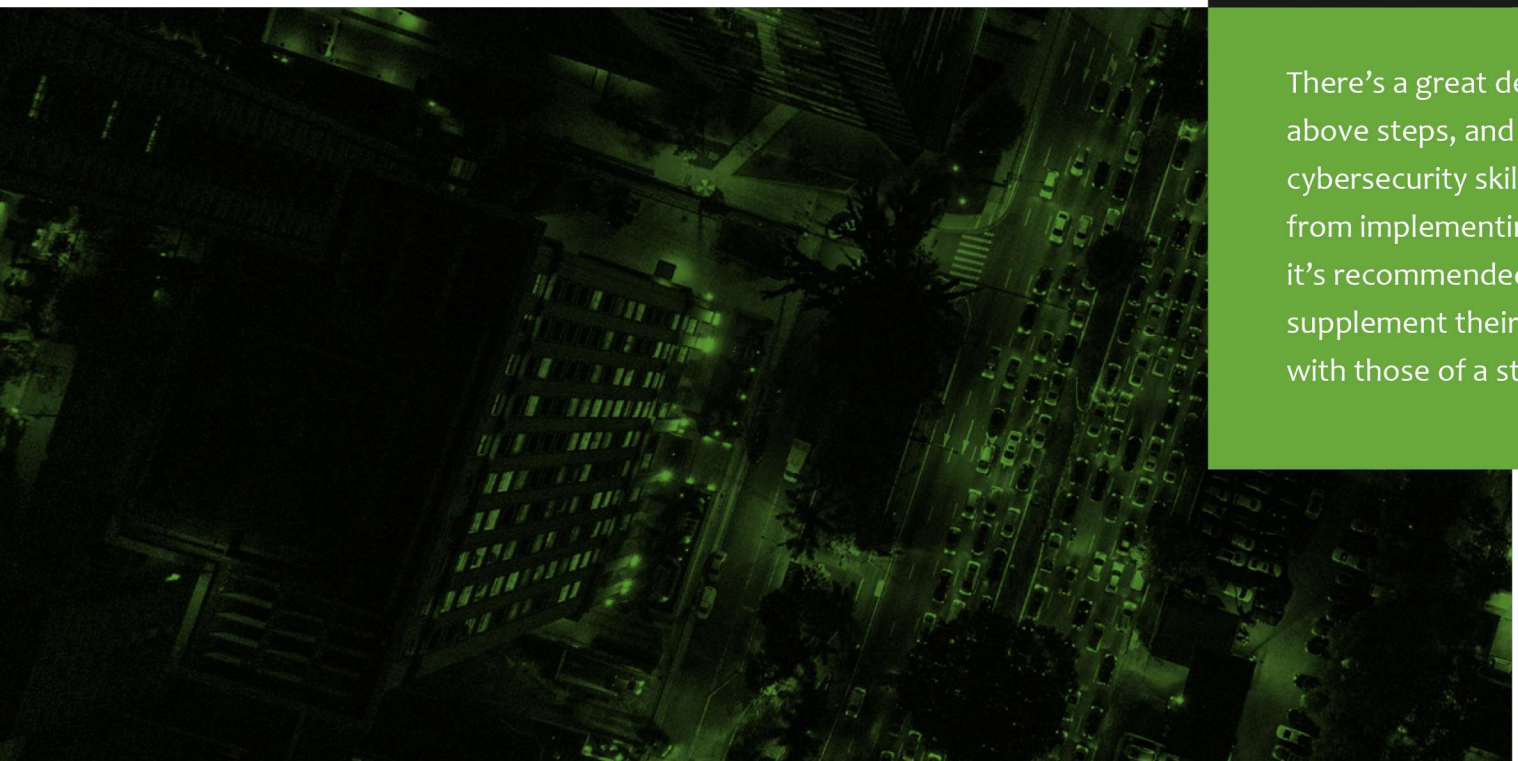
06 Maintain the Program

Program maintenance is continuous. Roles and responsibilities must be updated as resources change, and these must be tied to a job role. Additionally, the following activities should be reviewed and updated annually or upon change:

- ☑ **Data Inventory**
- ☑ **Risk Assessment**
- ☑ **Policies**
- ☑ **Standards**
- ☑ **Controls**
- ☑ **Procedures**
- ☑ **Plans**

How do you define "upon change"? If anything within the people, process, or technology categories change enough to introduce a new risk, that's when it's time to update relevant processes.

Remember:
You can't move into maintenance mode until you have a functioning program.

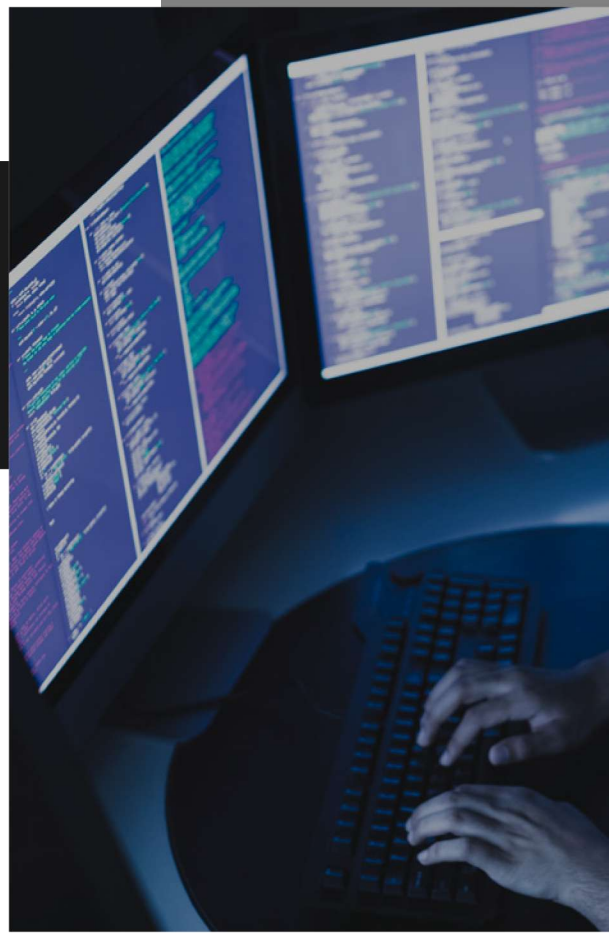


There's a great deal of nuance within the above steps, and you may feel that the cybersecurity skills shortage prevents you from implementing this strategy. Therefore, it's recommended for organizations to supplement their current internal resources with those of a strategic partner.

THE BENEFITS OF WORKING WITH A STRATEGIC PARTNER

The cybersecurity skills shortage is likely to get worse before it gets better.

How can organizations begin to address cybersecurity in a meaningful way, knowing they don't really have the resources to do it?



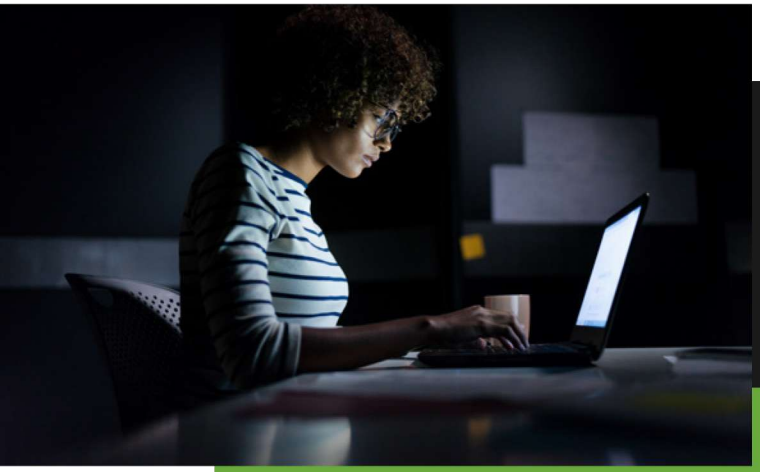
One potential solution is to engage with a strategic partner or trusted advisor. This can give your organization tremendous flexibility with both resource management and the optimization of workloads across functions. This approach can allow organizations to take the money they would've spent on one individual and divide it amongst a full team of experts to reduce the cost of initial effort, refactoring, and maintenance.

At GreyCastle Security, for example, we leverage this model to fit multiple experts into the same dollar amount. Essentially, we're able to "time slice" one individual into multiple skilled experts so that our clients have access to a full team of professionals.

Our experts are perfectly orchestrated to manage expanding workloads and the unique demands of our clients' risk profiles and cybersecurity programs.

There are different ways to engage with a strategic partner. Many organizations work with a trusted advisor on a one-time basis, such as for a risk assessment or penetration test. However, the more continuous your cybersecurity program can be, the more integrated it will become, the better the "on-demand" function works, and the more orchestrated your team of experts will be. When your cybersecurity program is managed and continuous, you'll see a greater return on your investments. This method is also better suited to the risks, threats, and problems we see in cybersecurity today because those are also continuous.

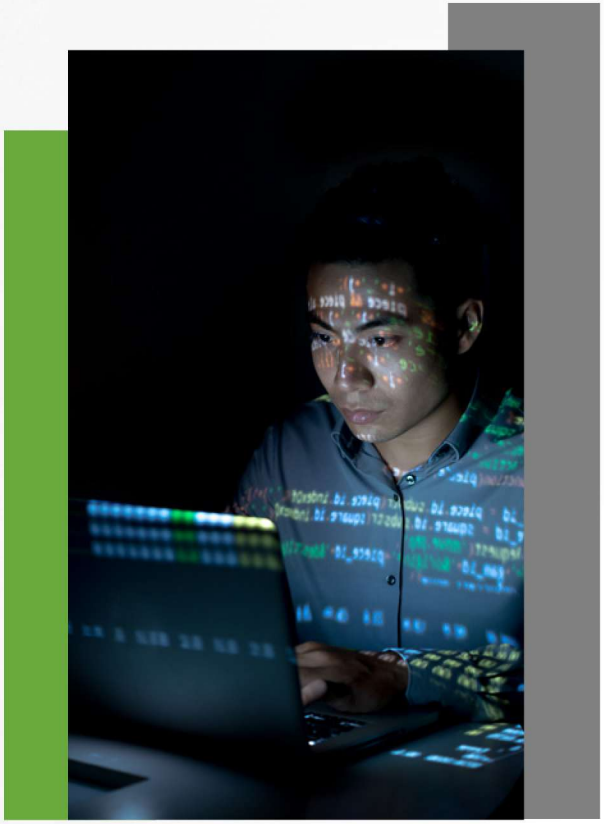
In today's environment, working with a strategic partner has become critically important. There's currently no end to the cybersecurity skills shortage in sight. The ability to find, hire, and retain cybersecurity talent today is a failed concept. Some may argue that large corporations are an exception because they have the capability to keep dozens or even hundreds of people on their teams. **But here's the rub: No matter the size of your team, it's never big enough to get things done.** Your team is always going to require assistance in specialty areas. There will always be peaks and valleys in workload and demand on specific resources. You'll also have to continue dealing with overhead and administrative headaches like hiring, retaining, and then replacing people when they leave.



Every dollar you invest in cybersecurity goes farther when you work with the right partner.

Interested in this approach? You might have a few questions. Below you'll find answers to some of the most common questions about working with strategic partners on your cybersecurity program.

What if I already have a CISO or cybersecurity personnel?



The honest answer is: It depends. Strategic partnerships that include a CISO tend to be effective because there's a full-time employee at the organization who's ultimately accountable, liable, and responsible for the success of the program. With that said, it's not a requirement to have a CISO to engage in a program. The reality is, no matter the size of your team, you'll face the risks brought on by the cybersecurity skills shortage, such as rising salary expectations and retention issues. **Thus, the question becomes: How does it make sense to augment your existing team?**

In the beginning days of an engagement, your strategic partner should leverage the institutional knowledge of your current staff to expedite and accelerate the process. Having someone within the organization who understands what's going on in the business from a cybersecurity perspective reduces the amount of time required for initial discovery. You want internal and external resources to become integrated as quickly as possible.

Having cybersecurity personnel on staff can help your strategic partners get up to speed faster. You've already invested in these individuals; a strategic partnership doesn't replace or displace existing cybersecurity resources. The partnership gives organizations greater flexibility into backfilling functions as existing team members transition into new roles or leave the organization. This arrangement works no matter what your team looks like today and can help you minimize the risk of attrition or additional headcount, and the challenges (and finances) that accompany that.

I've already done a penetration test and risk assessment internally. Do I have to reinvent the wheel?

Absolutely not. If you've done a standards-based risk assessment and built a roadmap from those findings, you can use these tools to build a cybersecurity program. The risk assessment is the cornerstone of the program you're building. If the risk assessment is sound, your strategic partner can move right into mitigation. If, on the other hand, you haven't performed a risk assessment or feel that it's either expired or not accurate, that's one of the most common places for a strategic partner to start. You want to be sure you're addressing things like compliance, security, privacy, certification, and board pressure equally. All the findings would be leveraged; there would be no wasted investment, assuming the work performed is accurate.

How much should I be spending on cybersecurity annually?

There's no "one-size-fits-all" answer for this. Instead, try thinking about the problem backwards. Let's say you're not spending anything on cybersecurity today. If you experience a negative outcome, whether it be a security incident or losing a customer contract, what would be the cost to your organization? What would be the cost of resilience (e.g., compliance resilience, security resilience) for scenarios that your organization is most likely to experience? Consider what it would monetarily be worth to you on an annual basis to potentially avoid some of those costs and reduce negative impact.

There's no one "right" number and there's no "right" percentage of your IT budget. Every organization is different and will have a different risk tolerance, board, and competitive pressures. Figure out what your organization can afford and what puts you in a defensible position. When you work with a strategic partner, if you calculate that you haven't spent enough or want to move quicker, you can increase your spend to accomplish business objectives.

THE BOTTOM LINE

If you could spend the same amount of money that you're currently spending on cybersecurity and gain access to an entire team of experienced subject-matter experts while increasing your ROI, would you do it?

Within this scenario, the amount of money you're spending doesn't matter—the methodology is flexible and scalable to an incredible degree. We live and work in an industry that's constantly and rapidly in flux. We may not be facing the same threats next month as we are today. The pressures we get from our board may change. The regulatory standards we need to comply with may be updated. All these things continuously change under us.

Don't you want to be in a position where not just your risk management function is flexible, but the methodology and delivery can change shape as the pressures change as well?

Hiring can only get a business so far. Organizations need to optimize their security functions in ways designed to streamline competencies and transform operational plans into revenue generators. A cybersecurity program isn't just about securing your assets. **It's an asset.**

The cybersecurity skills shortage means you need to think about your business in a new way. The nature of security is changing. Stop thinking of information security as merely a technical fix. Instead, approach cybersecurity from the perspective of solving specific business problems.

What does your organization want to achieve and what resources are necessary for success?

At the end of the day, we're all at risk. Organizations can't do everything themselves and they certainly can't wait years for the shortage to resolve to start thinking about security. Those that leverage strategic partnerships and build continuous, proactive cybersecurity programs will grow—even during a skills shortage.

GreyCastleSecurity.com

GreyCastle security

FOR MORE
INFORMATION ABOUT
GREYCASTLE SECURITY
AND ITS CAPABILITIES

GreyCastle
security

www.GreyCastleSecurity.com

518.274.7233