PLEXTRAC EBOOK

The Pitfalls to Establishing a Successful Cybersecurity Program

Avoid the approaches that prevent program growth and maturity.

PlexTrac®

Table of Contents

Introduction: Common Pitfalls to Effective Security

Focusing on pitfalls may seem like an odd place to start when considering how to shape a cybersecurity program; however, there are many easy-to-fall-into traps that can hold a program back both from functioning strategically and from getting the real cybersecurity work done. Examining what hasn't worked is an important first step in building something that does. As the adage goes, "Those who fail to learn from history are doomed to repeat it!"

Even seasoned professionals can fall into some ineffective patterns that make achieving a mature, high-functioning cybersecurity program a challenge. Pitfalls can cause difficulty even if they aren't catastrophic. Often what holds you back from having the control you want over your security posture is simply a lack of coordination of efforts and getting stuck in the grind.

It's so easy to get into routines and systems that appear to be working but that never help you actually grow and refine security. Seldom do cybersecurity programs have the financial or human resources needed to implement ideal solutions, not to mention adequate time to deal with the constant barrage of potential threats that is the norm in nearly every industry. But that shouldn't be an excuse to settle for the status quo— especially if that status quo isn't adequately protecting your organization.

Reevaluating strategy, tools, and priorities from the ground up can often uncover many ways to make better use of the resources already available. Creating a successful cybersecurity program isn't all about the resources, but rather how those resources are allocated and coordinated to get the right work done. But building a successful program first requires recognizing and climbing out of some common pitfalls you may have fallen into inadvertently.

Faulty approaches that will hold you back from real maturity include the following:

- **Maintaining a reactive program**
- **Measuring the wrong things**
- **Prioritizing program over people**
- **Neglecting business prerogatives**

Avoiding these pitfalls will establish a foundation on which to build a successful program. Gaining awareness of faulty practices and the strategies—or lack thereof—that have produced them is a necessary step in redesigning a program for efficiency and effectiveness.

Pitfall 1: Maintaining a Reactive Program

One of the most common approaches to defense isn't really much of an approach but rather a lack of a coordinated approach. Even experienced professionals can fall victim to constant reactivity—putting out one fire after the next but never getting ahead of the threats.

A FOCUS ON THE PAST

Unfortunately, simply maintaining a reactive program that focuses on legacy problems isn't sufficient to keep up with the consistent onslaught of cyber attacks. Perpetually dealing with the issues pointed out in the previous red team engagement—that probably happened a year ago—doesn't leave time for the present threats, let alone innovating for the future.

> **"...beware of getting stuck in a cycle that only addresses legacy issues from technical debt."**

Bad actors never rest, so neither can the good guys. Many programs struggle to gain a comprehensive, real-time view of their security posture or to be proactive and nimble enough to stay ahead of novel and even recycled tactics. While you may be constantly working to remediate problems, beware of getting stuck in a cycle that only addresses legacy security issues from technical debt. You must also plan for security in new projects and initiatives and stay ahead of the creativity of the adversaries.

Most programs are doing the right things, but not necessarily doing them frequently enough. The annual or biannual audit followed by the giant report that no one can ever quite get through is a cycle that can maintain but rarely strengthen an organization's security. Purple teaming that promotes better collaboration is becoming a more popular strategy, but even collaborative engagements are not enough if they only happen occasionally.

Shifting focus to the present—and future—requires having something to focus on. Identifying strategic goals with which to align team member priorities can help maintain a balance between cleaning up and completing older projects and proactively planning for new ones.

TOO MANY TOOLS

In addition to focusing on the backlog rather than the present issues, another easy trap is adding tool after tool without a strategy or plan for managing them all. This pitfall is two-fold: an uncoordinated cadre of solutions and adopting those solutions without clearly defined requirements or support.

The myriad of innovative tools, SaaS, platforms, and partners to address every aspect of performing and managing cybersecurity work is both fantastic and overwhelming. The pitfall is that it's easy to add one solution after another only to create more work than you started with. A patchwork quilt of solutions isn't necessarily going to keep you warm and safe when it comes to cybersecurity.

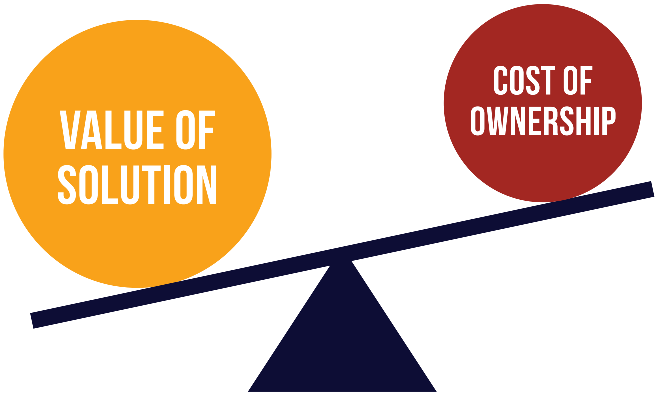
DOLLARS
COSTS
RESOURCES

Every product—even the open source, "free" ones—comes with a cost. That cost can include not only dollars, but also the human resources required for implementation, training, and sustaining the solution. Even managed services need an interlocutor, someone to be the boots on ground, which requires time and money spent on in-house human resources. Sensors need to be tuned continuously. Someone needs to be trained and able to respond to alerts. Automated patch deployment options need care and feeding. As the saying goes, "There's no such thing as a free lunch"—or in this case, a free solution.

Even if the cost is reasonable or only in the form of time and manpower, it can still be too steep an investment if your program isn't prepared to pay it. Programs, especially large ones with sufficient resources, can easily adopt new tools without properly analyzing the total cost of ownership weighed against the value the solution adds (or doesn't) to the program as a whole.

"Every product—even the open source 'free' ones—comes with a cost."

Failing to analyze the total cost of ownership for any given solution is setting the solution—and the team—up to fail. It is imperative that careful consideration be given to the value a solution can provide. A solution should provide value within the specific environment in which it will be implemented and be able to be coordinated with existing tools.



Pitfall 2: Measuring the Wrong Things

Even with a great set of tools in place, a program can still fail to achieve success if it isn't tracking the right things. The issue here is doing lots of work and managing lots of tools and having a false sense of security because you lack a real-time view of the environment.

COMPLIANCE AS AN END IN ITSELF

Security frameworks and compliance matrices are excellent guides to best practice, but achieving compliance doesn't necessarily mean you are secure. When meeting compliance is the end all be all, the focus is often more on ticking boxes than attaining real security. In other words, the external measurement of meeting compliance standards can become more important than thoroughly analyzing the actual security in a given system.

Frameworks can provide a false sense of security depending on how you use them and what it takes to satisfy auditors or leadership. The pitfall here isn't the framework itself or the external accountability of achieving compliance to a set of regulations, but rather using compliance as the measure of security.

Putting a control or tool in place to satisfy a regulation and calling it good isn't really the point. Just having an automated scanner, for example, doesn't mean much if you aren't consistently analyzing the scanner results and identifying and remediating issues.

Avoiding this situation may seem obvious, but the pitfall is, unfortunately, common in the overworked, under-resourced environment of many security teams. It can be easy to satisfy outsiders that compliance boxes are checked while still remaining far behind in enacting measures that really ensure a secure environment—which is the actual purpose of the regulation anyway. When you have an accurate and real-time view of your environment and programs and systems to actively and promptly respond to threats, chances are you are already living into best practice frameworks and meeting compliance standards. The opposite, however, is not necessarily true. Don't put the cart before the horse.

> **"Frameworks can provide a false sense of security depending on how you use them..."**

LACK OF ENVIRONMENTAL AWARENESS

It all comes down to environmental awareness. You can't secure or remediate what you aren't aware of. Unfortunately, it's difficult to gain a real-time view of all perimeters, especially Internet of Things devices. Many teams accept a dated or limited view of their environment because they have their hands full dealing with the issues they already know about.

However, gaining a real-time view of all vectors is not the place to settle or skimp on efforts. You can prioritize what threats or weaknesses to deal with, but you can't block attacks in areas you aren't watching. Constant remediation is just busy work if you aren't remediating the right things. The path to maturity begins with knowing yourself. The path to a mature program begins with knowing your environment.

Pitfall 3: Prioritizing Program Over People

Cybersecurity professionals are not often perceived as people-persons. Obviously this is a huge stereotype, but if this stereotype is true for you or the members of your team, you might be more likely to fall into the pitfall of prioritizing your program over the people in your organization.

According to study by IBM Security and the Ponemon Institute, 90 percent of all cybersecurity breaches are a result of human error. This is a massive statistic that simply can't be ignored by security programs that want to reach their goals.

All the systems and tools in the world won't make up for the human factor in achieving security. Failing to gain buy-in from users who either ignore or can't manage certain features is a sure fire way to doom a program from the start.

A SECURITY DICTATORSHIP

You might remember back in the late 1990s Jimmy Fallon's ongoing Saturday Night Live character Nick Burns, your company's computer guy. This obnoxious IT specialist would come to the rescue of the average company employee who was having computer issues sporting acerbic arrogance and spewing technical jargon, solving the problems while demeaning as idiots everyone along the way. While the dated technology in these skits adds a new level of humor, the primary joke is funny and current because it is so often true.

IT professionals in general and cybersecurity experts in particular are obviously not all arrogant jerks, but their knowledge and expectations can be intimidating to the average employee. On top of feeling intimidated, employees often label the security department as the "Office of NO!" because the security department so frequently shuts down approaches to problems or tasks outside of its own. In short, employees often feel security policies and procedures hold them back from getting their work done in efficient ways.

The pitfall in the above scenarios is running a program that alienates people who should be allies. When the IT department is only seen as the place that criticizes your every move, forces attendance at unending training sessions, demands adherence to laborious and unrealistic practices, and defaults to "NO," you'll be hard pressed to get the buy-in necessary to achieve real success across all vectors. Rather, successful teams must develop a culture of collaboration that empowers departments throughout the organization to achieve their various missions securely.

NO

👎

The infosec department is seen as a group that criticizes your every move.

YES

👍

The infosec department is seen as a group that actively protects your assets.

UNREALISTIC SOLUTIONS

Another big mistake in dealing with people and cybersecurity is underestimating their creativity and motivation. And we're not talking about their innovative strategies to protect the organization from virtual attack, but rather their ability to circumvent controls and policies to get their work done. When the employees in an organization see information security solutions as barriers to their work—especially if they don't understand the importance—they will find workarounds.

The pitfall is pushing security solutions that fail to account for the humans trying to implement them. Every employee has their own priorities based on their individual roles. Unless they work in IT, their priority is not likely to be cybersecurity. Just assuming that people will change their priorities because of a security policy or best practice can lead to poor implementation. A better plan is to find and create solutions that can be realistically adopted.

"When the employees in an organization see information security solutions as barriers to their work—especially if they don't understand the importance—they will find workarounds."

The classic example of this issue is password best practices. While a random, unique, memorized, 33+ character password that consists of every letter, number, and symbol on the keyboard is undeniably the best way to protect an account, demanding that all employees use one just isn't realistic. Forcing this kind of policy has usually resulted in less universal—and certainly less controlled—adoption, like that password written on a sticky note posted on the monitor. In this example, deploying a password management solution is a reasonable middle ground to enforce strong security policy and avoid bad habits from users.

Users will find ways to get their missions accomplished. Successful security measures enable operations, or, at a minimum, don't present insurmountable obstacles that encourage secret insurrection.

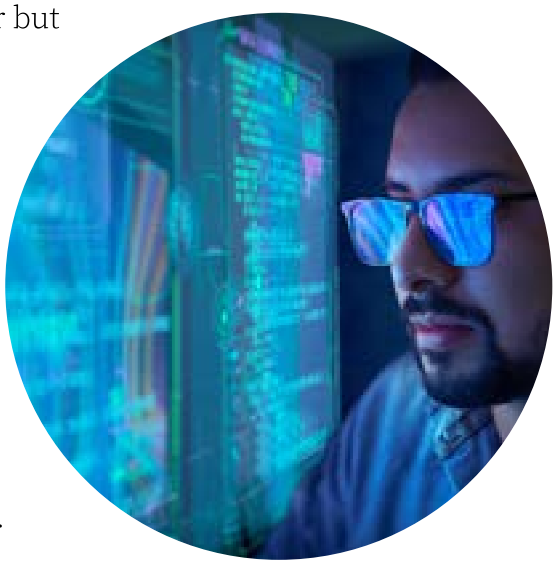
Pitfall 4: Neglecting Business Prerogatives

In much the same way that failing to account for people in security planning will torpedo success, so will neglecting to tailor the security program to the goals and culture of the organization. Companies exist to provide a product or perform a service, and, ultimately, to make money doing so. They don't exist to be secure, rather cybersecurity should enable the business to do whatever it exists to do.

When security solutions impede the ability of the organization or individual employees to effectively do business, the program has failed in its purpose no matter how well it's protecting the crown jewels.

SECURITY PLANS OVER ORGANIZATIONAL GOALS

Concentrating only on security without fully considering functional business operations and goals will ensure a plan that looks good on paper but won't live up to expectations in reality. The pitfall is building a security program— even an exceptional one—independent of the company it's supposed to protect.



A security program that doesn't adequately account for organizational goals and culture may look really great and meet compliance requirements, but it won't be sustainable. As security policies come in conflict with business agendas and processes, adherence to the policies will inevitably dwindle.

Successful programs start by identifying organizational priorities to guide infosec decision making and then build trust with leadership to ensure supported implementation.

PERFECT INSTEAD OF GOOD

One sincere but misguided practice is demanding perfection from solutions and people. Information security is a part of risk management, not risk elimination. Therefore, implementing solutions that are iron clad but get in the way of the actual work of the organization are not nearly as effective as less perfect but more manageable options.

When new administrative and technical controls are put into place without a proper analysis of the business impact, there's a good chance they simply won't work. In the same way, sweeping policies that haven't accounted for necessary exceptions aren't likely to gain universal buy-in. And while your organization may have processes in place to formally approve exceptions to policy, users don't want to deal with more hoops to jump through.

Even the best policies are only as strong as the ability to enforce them. Perfect can be the enemy of good. Good security is achievable; perfect security is not.

> **"Companies exist to provide a product or perform a service, and, ultimately, to make money doing so. They don't exist to be secure, rather cybersecurity should enable the business to do whatever it exists to do."**

Conclusion: A Foundation for Success

A mature cybersecurity program is measured by its ability to successfully manage risk unique to the environment. In today's world, it isn't a matter of IF you're breached, but WHEN you're breached. You may even be breached right now. It's not a lack of breaches that proves an effective program, but rather how quickly the actions of the attackers can be detected and remediated.

Security is hard. We all know this, but by working smarter (and maybe a little harder) you can put your best foot forward in your quest for improved security posture. Avoiding dangerous pitfalls like maintaining a strictly reactive program, measuring the wrong things, prioritizing your program over your people, and neglecting organizational goals and culture is a great start.

A clear, unflinching and continuous assessment of current practices and the subsequent policies, processes, and tooling choices they will produce is the only way to break out of one cycle to try something new. Once you have stopped relying on the wrong things, you are ready to build a program and see it to maturity based on an effective strategy.

Implementing an effective strategy rather than just maintaining the status quo requires constant management. PlexTrac is a comprehensive solution for managing all aspects of a cybersecurity program that enables professionals to focus on the right things and get the real work done.

From providing a real-time view of security posture to managing data and analytics to enabling communication and collaboration within the team to reporting to leadership, clients, and constituents of all levels, PlexTrac is truly a platform for all security professionals and all security programs.

Learn more about the PlexTrac solution for managing your security program.

SCHEDULE A DEMO TODAY

PlexTrac is the premier penetration test reporting, collaboration, and management platform designed to automate planning, documentation, communication, and remediation tracking, allowing service providers to enhance margins and client outcomes and enterprises to demonstrate the value of internal pentesting efforts and improved security posture.

www.plextrac.com

PlexTrac®