

PLEXTRAC EBOOK

The Pillars to Establishing a Successful Cybersecurity Program

Key strategies behind mature and functional programs

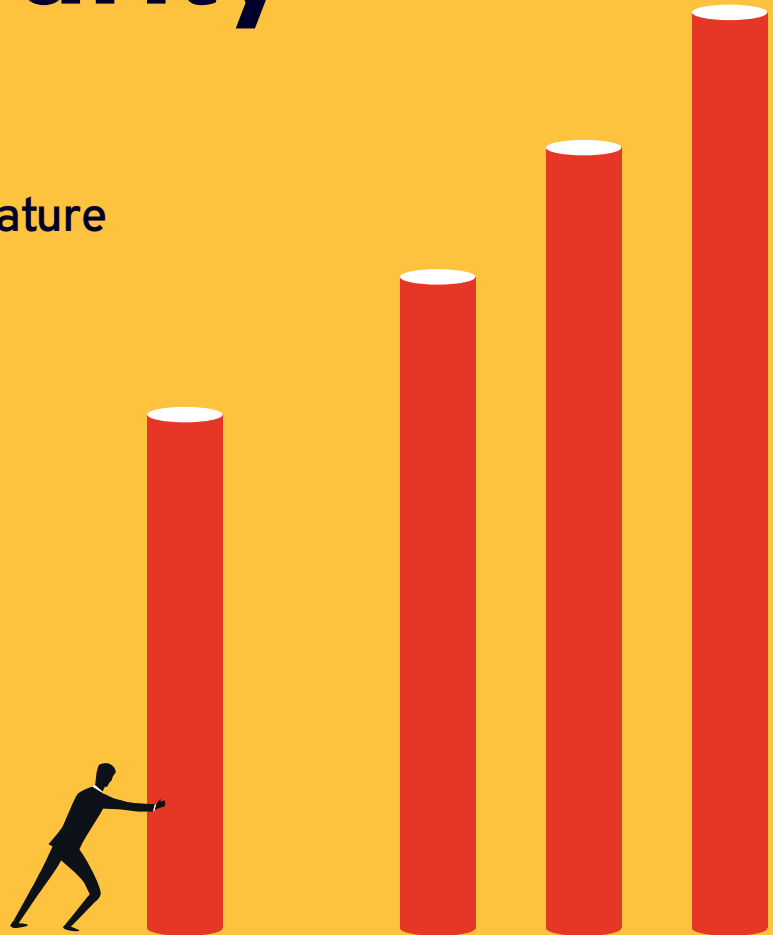


Table of Contents

Measuring Maturity 2

Building Around the Pillars 3

 Developing a Proactive Paradigm 3

 Understanding the Environment..... 6

 Investing in Corporate Culture 9

 Accepting Enterprise Risk 11

Moving from Theory to Action 15

 Establishing a Baseline..... 16

 Demonstrating Improvement 17

 Setting Achievable Benchmarks 18

Quantifying Success..... 19

Measuring Maturity

Establishing a successful, mature cybersecurity program requires building upon a foundation of best practices. Whether your security program has been established for a long time or you're just getting started, it's important to take a moment to step back and focus on the bigger goals of the program and the foundational pillars that must be in place in order to achieve those goals.

That kind of talk sounds good, but isn't that what we are all trying to do everyday anyway? And what exactly are the pillars of an effective cybersecurity program? Every acronym-ed organization and framework from NIST to DoD to ATT&CK seems to offer different definitions on what the pillars to success in information security really are. It can all become confusing and more than a little bit exhausting.

Although there are a lot of differing viewpoints on the pillars of cybersecurity, they are mostly variations on the same theme. Experts across the board really do share a set of common principles in their advice on effective security management. The challenge lies in understanding the philosophy behind the tenets and making them actionable to achieve your goals.

Dwelling on philosophy can seem like a dangerous prospect in an industry characterized by constant and very tangible threats; however, starting at the conceptual level is essential when attempting to build a program that actually works. Otherwise you can spend a lot of time—and a lot of money—working in circles.

No matter where your program currently stands, enhancing your maturity requires both the theoretical foundation and an actionable implementation plan:

- 1. Fully understanding best practices or industry “pillars,” and**
- 2. Taking action to align policies and practices to the pillars while accounting for organizational goals.**

Building Around the Pillars

The pillars we offer are a multifaceted philosophy more than a checklist of strategies or a toolbox of solutions. Implementing these principles will look different in every context and require different strategies and tools depending on organizational goals. However, for a program to be comprehensive and truly effective, these four pillars should serve as the cornerstones.

Developing a Proactive Paradigm

The first pillar is all about living in the present and consciously building a program around the needs of the environment. Not everything can be a top priority, so it is important to choose what areas will be and to make choices about systems, tools, and policies that will help you meet goals now and into the future.



Constructing a program around a proactive paradigm requires strategic consideration of the problems your organization is most concerned about and the best ways of addressing them now and over time. Being proactive means you are in the driver's seat rather than adversaries. Sure, breaches are always possible, but anticipating your weaknesses and resourcing the most important areas reduces their potential for occurrence and impact.

IDENTIFY PROBLEM AREAS

You can't follow a map if you can't identify your current location. The first step in developing a proactive paradigm to guide a security program is determining

where to focus efforts. What are the problem areas and which are priorities?
Where would a breach hurt the most?

Not everything is of equal importance so don't treat it as such. Avoid spreading resources too thin over too large an attack surface. This advice doesn't mean that you neglect your view of the whole attack surface, just that not every area is covering data of equal value. You have to know the environment to determine strengths and vulnerabilities.

Being proactive in your approach means thinking like the adversary. What are the most desirable assets and what are their vulnerabilities? Don't wait until after a breach has occurred to consider these questions. Running tabletop exercises on a regular basis, for example, can help your team consider scenarios and address problems BEFORE attacks occur. Environmental awareness and strategic defense are hallmarks of a proactive approach.

ESTABLISH GOALS

Once problems are identified and prioritized, you can establish baselines and set goals. Goals are forward looking in nature and that's what a successful program should be too.

Without specific measurable goals, it's easy to spend all your time and resources putting out existing fires, even if that damage is done and over. Learning from past breaches is important, but you won't even do that unless you make time to consider them in light of strategic priorities.

“Without specific measurable goals, it's easy to spend all your time and resources putting out existing fires.”

INVEST IN PROPER TOOLING

Part of adopting a proactive mindset means finding the tools that will help you meet your goals rather than continuing with legacy solutions or adding tool after tool

aimlessly. Your process and context should drive tooling, not the other way around. But you can't really determine the best solutions until you've identified weaknesses and priorities.

You should start with an analysis of the value of existing solutions. Why did you invest in a solution? What was the problem you were trying to solve? Has the solution solved, or at least mitigated, your problem?

If not, you should not assume the solution itself is to blame. Consider if you have invested the time in training your team to implement and sustain the solution. Are you using all the capabilities of the solution that you have already paid for?

If you have truly given a solution the appropriate resources and it is still not solving your problem, it's time to take a step back. Just because it was a problem you devoted resources to before does not mean that it is currently your top priority. Sometimes you no longer need the bandaid—and sometimes you have a new wound that is more pressing. The bottom line is that if a problem still exists, it should be put back into the pool of problems and prioritized accordingly. It should get no special treatment because it was previously addressed.

The best security tools for your organization will help your strategic initiatives move forward. They will help resources stretch rather than cost more than the value they provide. They will improve efficiency allowing you to spend more time on your priorities.

Every context will require different tooling based on the make up and maturity of the program. That's okay. The key is to analyze your environment first, identify problems, set reasonable goals, and then determine what combination of products, programs, platforms, and partnerships are going to provide the most value for your context.



Understanding the Environment

To build a program strategically, it is essential to fully understand the environment. To understand the environment, you must measure the right things. Not only do you need to have continuous and real time data, you also must analyze the data to provide an accurate picture of the attack surface you are protecting. Without a thorough and accurate grasp of the environment, defenses will always be vulnerable.

GAIN A REAL TIME VIEW OF SECURITY POSTURE

The trouble with understanding your environment is that the environment is always changing. Nothing is static in cybersecurity so your view can't be either or you'll always be focused on the past instead of the present. Analytics are key to gaining a real time view of security posture.

First you have to collect the massive amount of data that your system is continuously producing—but just having the data is not enough! You also have to be able to rapidly aggregate and analyze the data into meaningful information that can inform your decision making.

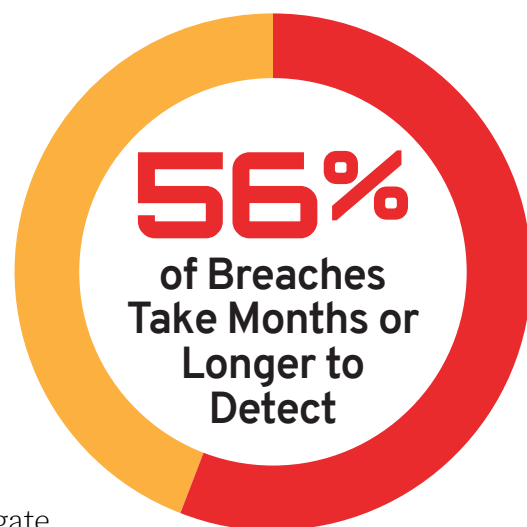


Once you have the analytics available, they can serve an invaluable tool for allocating resources and advocating for more. They can inform goal setting, communicate powerfully to constituents, and, of course, flag breaches and reveal vulnerabilities.

TRACK THE RIGHT METRICS

All the data and analytics in the world won't help improve security posture if you aren't tracking and prioritizing the right things. Measuring the raw number of vulnerabilities remediated provides data—and you certainly want to see that number rise. However, how long is it taking to remediate those vulnerabilities? Are you prioritizing your efforts on the critical assets?

Mean time to remediation (MTTR)—the time it takes for your systems and people to detect, respond, and remediate—is a critical metric and fairly easy to measure. However it can also be misleading if all your assets are considered together. If you patch a low severity vulnerability on 1000 desktops in a week, but a critical remote-code-execution vulnerability languishes on your domain controller for months, your MTTR number in aggregate may hide the true level of organizational risk.



Source: Verizon's 2020 DBIR

You should group your assets by their criticality to your organization. Consider the impact of a breach on current operations and strategic viability. Then establish benchmarks for your MTTR based on the group and write policy that codifies these benchmarks as internal service level agreements to set performance expectations. For example, you may set your internal SLAs so that all high or critical severity vulnerabilities impacting critical assets should be remediated within 72 hours. Lower severity vulnerabilities impacting less important assets may be granted much longer windows for remediation.

The point is not only to be tracking data but also to use it effectively to determine priorities. The 2020 Verizon Data Breach Investigations Report states that 56 percent of breaches take months or longer to detect. Considering how long it takes just to get to the point of detection in many cases, you must consider MTTR holistically in order to really manage risk.

VALIDATE EXISTING PROCESSES AND TECHNICAL DEFENSES

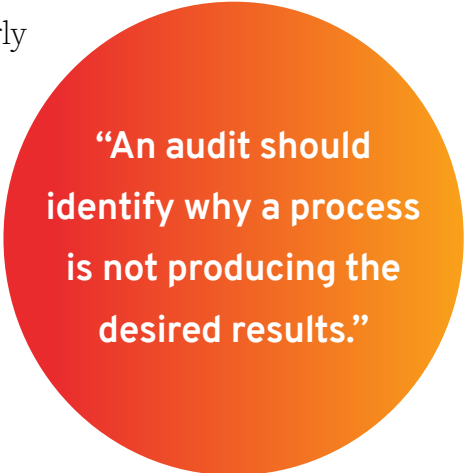
Unless you are building a program completely from scratch, you undoubtedly have existing processes in place. Are those processes being regularly performed, and are they producing the desired results?

To answer this question truthfully requires audits. “Audit” is a dirty word in some environments—if it is in yours, then you are not handling the results properly. An audit must go beyond simply determining whether a process is being performed and assigning blame if it is not. An audit should identify why a process is not producing the desired results. Are there technical blockers? Perhaps training or other human resourcing issues?

While audits are appropriate for discovering problems with process, they may not be able to uncover technical problems. You can have a well-functioning process to perform continuous monitoring of SIEM alerts. However, if the alerting rules are not properly tuned or the proper data is not being ingested by the SIEM, the process is not producing the desired results. This situation is where regular testing is important.

Most programs participate in evaluation occasionally but that isn’t nearly enough to maintain an accurate, up-to-date view of security posture. Frequent iterative cycles of audits and testing are necessary to really determine what is working and what needs tweaking.

A “set it and forget it” attitude in cybersecurity is dangerous. Instead, successful programs foster regular rhythms validating if solutions are working for the environment and verifying that the solutions are doing what they are supposed to do—and changing them when they aren’t.



“An audit should identify why a process is not producing the desired results.”

Investing in Corporate Culture

Successful security programs don't happen in a vacuum. Rather, they account for their environment, and a huge part of any organization's environment is the employees. Managing the human element of cyber interactions is imperative to comprehensive security.

The infosec department must take the initiative in building positive relationships outside of the team and for training everyone in the organization on good cyber hygiene. Everyone at every level can be a defender or a liability. This pillar recognizes the role of the cybersecurity specialist in navigating the complexity of bringing solutions and the people that use them together.



Cybersecurity Specialists:
Navigating the complexity of
bringing solutions and the people
that use them together.

WIN FRIENDS...

Dale Carnegie's classic self-help book *How to Win Friends and Influence People* is a must read in many college business programs. It should be for computer scientists as well. Most security practitioners didn't get into the field because they wanted to exercise their people skills. However, they sometimes seem to forget that average employees didn't take on their roles because they wanted to specialize in cybersecurity.

If properly equipped, the people of your organization can be the first line of defense against breaches. Investing in all employees as if they are vital members of your security team will reap huge returns.

Part of winning friends among all constituencies means making the IT department helpful and approachable—not intimidating and burdensome. For example, employees can be allies who report suspicious activity or admit when they’ve fallen for a phishing attempt or they can ignore and hide what they see and do for fear of reprimand. Successful programs have managed the latter through investment in employee-friendly policies.

...AND INFLUENCE PEOPLE

Building positive relationships with constituents and accounting for organizational culture in making policies and choosing solutions doesn’t equate to relaxing security standards. The benefit of a cooperative approach is that buy-in for the policies and procedures will be much higher.

If 2020 has taught us anything it’s that employees are resourceful and resilient. Smart cybersecurity programs will use this to their advantage by compromising to find workable solutions. For example, password vaults are not without security concerns but they have a low barrier of acceptance and make security easier for the average employee.

Compromising to find acceptable, albeit perhaps imperfect, solutions that will engage people from all levels of the organization is going to be more effective in the long run and gain credibility with stakeholders when more difficult measures are necessary.

TRAIN AND ENGAGE

A proactive approach is as necessary in working outside the IT department as it is within. Training and engaging everyone at all levels of an organization on security best practices and company specific policies and procedures must be a priority.

Sending out required virtual training sessions on phishing and social engineering is great, but it may not be enough. Eliciting real engagement that motivates habit change usually requires relationships and ongoing communication between the security team and the organization in general.

Think of everyone as security gatekeepers that can directly help or hinder your program success and then equip and empower them accordingly. Engaging everyone as security gatekeepers for the organization will entail providing information and explanation not just directives, making context and choices available rather than considering everything “need to know” only, and communicating in layman’s terms rather than industry jargon.

“If 2020 has taught us anything it’s that employees are resourceful and resilient. Smart cybersecurity programs will use this to their advantage by compromising to find workable solutions.”

Accepting Enterprise Risk

This may seem like a strange concept as a pillar of cybersecurity, but the reality is that doing business of any kind requires taking risks. Information security is a function of enterprise risk. The cost of doing business, going to school, offering medical care, and nearly everything else in our modern lives entails information security risk.

Successful security programs recognize the inherent risk in their industry and organization and account for it in their strategy, processes, and communication. Accepting the risk of doing business and leveraging security strategies to mitigate that risk and accomplish organizational goals is the real purpose of a cybersecurity program in the first place.

PRIORITIZING THE ORGANIZATION'S GOALS AND OBJECTIVES

Unfortunately, security professionals can become so hyper focused on security best practices, infosec industry trends, and achieving ironclad perimeters that they can forget that they exist not as an end in themselves but rather to enable an organization to do its work. The organization's goals and objectives should drive the security program, not the other way around.

A recent Trend Micro study found that only 23 percent of organizations prioritize the alignment of security with key business initiatives. Although this problem is certainly a two-way street, the infosec department must do its part to effect change and create urgency for organizational leadership to be actively engaged in cybersecurity policy and practice.

When constructing a security program, the foundation should be built on a thorough analysis and understanding of not only the industry the program is operating in but also the microcosm of the specific organization. Any compliance requirements should, of course, become a baseline for security strategies but so should the culture of the specific business within its industry.

Analyzing the organizational culture and goals and how security practices can be leveraged to ensure the business is achieving its ends will, in turn, ensure the security program is supported and successful.



COMMUNICATE EFFECTIVELY

For a security program to serve the organization well, communication with all departments and levels is necessary. The security team must hear from the departments and leadership to understand the priorities and challenges they are

facing. The security team must also effectively communicate with departments and leadership what is necessary from a security perspective to support and protect them.

Effective communication means providing information in a language the user recognizes. It's hard to gain buy-in on something you don't fully understand, so the job of the security professional is to learn to translate technical jargon and analytics into clear and persuasive reports. And security experts can't just expect people to take their word for it on expensive or difficult solutions. Evidence is also essential to effective communication, and security professionals need to be able to provide it and to justify their decisions and requests.

Part of making the goals of the enterprise central to the security program is building bridges between organizational leadership and the information security department. Doing this means trusting that leadership—when provided clear information—can make decisions regarding security that are good for the organization as a whole.

BUILD TRUST

If the security department wants to gain the support of leadership at all levels, the onus is on the security department. Part of building a successful security program is building trust and gaining buy-in with all constituents for security policies that affect them.

Clear Communication:
Key to any successful
cybersecurity program.



“Part of making the goals of the enterprise central to the security program is building bridges between organizational leadership and the information security department.”

Building trust requires operating with transparency about successes and failures. It requires taking responsibility even when the powers that be may not fully comprehend the situation. It requires reporting out your work regularly and in forms that leadership can understand.

CONCLUSION

The four pillars discussed here are interdependent. Without proper attention to all four, your program will struggle to stand. Together they can guide cybersecurity best practices within the infosec department and the organization as a whole.

Adopting the four pillars means strategically designing a program around the environment and organizational context to best prioritize activity and allocate resources to achieve security goals—and, ultimately, success of the organization in achieving its goals.

But strategy must be put into practice and theory must become action for a program to really make strides. The pillars are the strategy and theory that inform and guide; they are not the techniques or tools that are used everyday to get the security work done. Once you've considered the pillars within the context of your program, you can move on to the practices that will enable you to accomplish your goals.



Moving from Theory to Action

Although practices like employee awareness training, vulnerability management, monitoring, response, assessment, and audits are essential, they are not pillars but rather techniques you use to meet specific objectives. To put the pillars into action involves more than implementing a set of techniques. First you must identify specific objectives, and those objectives should be derived from goals.

For the implementation of specific practices, and even more so, the tools to support those practices to be effective in achieving objectives, you must have realistic and clearly defined goals. Once you know what you are trying to achieve, you can implement the appropriate practices to get you there.

Goal setting, and then monitoring, measuring, and adjusting the goals as the program matures, are the keys to putting the pillars into practice.



1

**Establishing
a Baseline**



2

**Demonstrating
Improvement**



3

**Setting
Benchmarks**

Establishing a Baseline

So what should the goals of a successful cybersecurity program be? The easy answer is breach avoidance, but that may not fully encompass a program's goals. Goals need to be tailored to the level of maturity of the program.

Maturity of a security program is not equal to the size of the organization. Programs of all sizes and resources can be more or less mature. The prerequisite to effective goal setting is honest assessment of the current state of the program to establish a baseline to work from.

Goals should not be geared towards achieving particular values until you have a clear understanding of the current environment. For example, it isn't realistic to set a goal of having 95 percent of systems patched against known vulnerabilities within two weeks if you have no idea how many unpatched systems you have today or how long it is taking to patch them.

Determine what you are currently doing and where you are lacking. Once you know what you know and what you are capable of doing, you can set reasonable goals for improvement prioritized according to both your program's capabilities and greatest threats.

Key questions to answer to determine a starting point for goal setting include the following:

- **Are you performing vulnerability management?**
- **Where have you been attacked in the past?**
- **What are you protecting?**



Demonstrating Improvement

Once you have established a baseline, the next step is prioritizing and determining how you will measure success. Part of effective goal setting is being able to gauge when you've reached the goals. Goals must be specific, measurable, and attainable.

After you've assessed the existing program's vulnerabilities and prioritized what data needs the most protection, identify key areas to focus improvement efforts. You won't be able to tackle everything at once, so determine the most significant places that you can move the needle with the resources you have.

Next, determine what metrics you will use to assess whether efforts are effective. Keep in mind that achieving a goal doesn't have to mean reaching a specific number but rather moving toward positive change. Choose metrics that can help demonstrate progress and that are meaningful for whatever it is you are tracking. All progress has a cost in dollars and resources. Be sure to set up methods for figuring out your progress to cost ratio.

Finally, determine who will be accountable for what in your goals and objectives. If it isn't someone's job, it won't get done. Match every objective toward a goal with the practices it will take to meet it. Then consider what will need to happen to maintain those practices. All team members should know their part to play in the daily work that will collectively push the program forward.

Key questions to answer on how to demonstrate movement toward goals include the following:

- **Where will you focus?**
- **What metrics will you use?**
- **Who is accountable?**



2 Demonstrating Improvement

Setting Achievable Benchmarks

Goals should not be stagnant. Maturity comes from progressively meeting benchmarks and striding towards new ones. First and foremost, goals for your security program should be realistic to your baseline, then concrete and measurable. Goals like this can be accomplished and expanded or replaced in natural cycles.

Forward looking goals will be supported by planning and budgeting. When you can consistently meet benchmarks and set new ones, you can also begin planning ahead and advocating for resources to continuously up the ante. Demonstrable progress is easy to get behind. Setting realistic goals, achieving them, and measuring your progress will make a strong case to leadership to approve requests for more or better tools, more personnel, or whatever else might be needed to keep up the progress.

The best part of establishing a cycle of progress is that you will begin to have a better idea of what you actually need to be successful and the evidence to support it. To that end, the final step in goal setting is an ongoing one. You must be continuously evaluating priorities, evaluating solutions, and evaluating success—and adjusting your strategy accordingly.

Key questions to answer on how to measure success include the following:

- **Do you have defined measurements?**
- **Are you planning for the future?**
- **Are you continuously evaluating?**



3

**Setting
Benchmarks**

Conclusion: Quantifying Success

A thorough analysis of a program to understand the challenges it faces and the stagnant processes it may be relying on is the first step to maturity. The next step is using contextual understanding to construct new policies and processes around the pillars of cybersecurity. Finally, devising informed goals and continuously monitoring progress will move theory to practice to achieve success.

The level of security management described above is sophisticated and difficult. It is also essential to maturity. You won't conquer it overnight and you don't have to get there alone. The PlexTrac solution is a comprehensive cybersecurity management platform that addresses all four of the pillars.

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 at plextrac.com.

 **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 © 2023 PlexTrac, Inc., all rights reserved.

