PRAETORIAN

WHITE PAPER

The Elephant in the Room: Why Security Programs Fail

Understanding common root causes of strategic failure and how to evolve to a more effective, risk-informed program

INSIDE THIS REPORT

Based on Fortune 500 security assessments

www.praetorian.com

INTRODUCTION

The Uncomfortable Truth

Many organizations will struggle and ultimately fail to keep a sophisticated attacker from breaching core assets. This is often despite significant effort, expertise, and investment.

At Praetorian, we have the privilege of working with clients across the Fortune 500, and we have observed this harsh reality play out repeatedly, even for organizations with substantial security programs. More often than not, our security engineers are able to compromise the crown jewels of our clients in as little as a few hours, and not more than a few weeks.

The fact that our small teams achieve these results points to a sobering likelihood—better-resourced nation-states and criminal organizations are able to achieve similar results.

Too much time and money is spent on things that do not appreciably reduce risk.

Through the course of client discussions over the past three years, Praetorian has come to the belief that many security programs spend too much time and money on activities that do not effectively improve outcomes. Lots of effort, insufficient results.

ANALYSIS

Factors Contributing to Inefficiency

A number of factors contribute to security program inefficiency, including but not limited to:

- **Blind adoption of frameworks** - Relying on frameworks and compliance regimes without sufficient attention to the organization's unique risks and threat profile
- **Divergence from evolving risk** - Stagnant organizational priorities and metrics-tracking from ever-evolving risk
- **Performance vs. effectiveness** - Focusing on security controls rather than securing assets
- **Inadequate verification** - Failing to sufficiently verify that security controls were implemented properly and function as intended
- **Organizational stovepipes** - Diffusion of roles and knowledge leading to underlaps and overlaps in controls and processes

Happily, the above are solvable problems. From the same conversations with many clients, we have also seen common characteristics of those security programs that are able to keep an advanced attacker out or quickly shut one down.

> **Organizations that remain focused on their unique risks and implement matching effective controls can build highly capable security programs.** These teams tend to be agile and adaptive, and often carry a lower cost:revenue ratio than most organizations.

FOUNDATION

Three Fundamental Premises

Before going further, there are three core premises that underpin much of this paper. If you disagree with these, you may disagree with the remainder of the paper and its conclusions.

1. The Mission is to Reduce Organizational Risk

A cybersecurity organization's mission is to reduce the likelihood of security incidents and reduce the costs associated with an incident should one occur. The mission isn't to keep an attacker from breaching the perimeter—those are means to an end.

2. Words and Framing Matter

The words and thought patterns we use to define problems influence the solutions we develop. Many organizations use frameworks that are years old in an unsuccessful attempt to grapple with a chaotic reality.

3. Leaders Must Identify the "Right Things"

The "Right Things" are activities that will reduce the organization's risk most efficiently. The challenge is that there will always be multiple right things, and they will shift over time.

The reason security programs ultimately fail is they have focused on the wrong things or tried to do too much.

PART I

Activity Without Outcome

How Did We Get Here?

The most common thread we have seen amongst well-resourced security programs that ultimately fail is not that they haven't done enough. Instead, it often seems that they have focused on the wrong things or tried to do too much, leaving key controls incomplete.

A distinction needs to be made between activity and results. Unfortunately, we see a lot of well-intentioned, well-resourced security organizations that are engaged in a lot of activity, but that activity hasn't reduced the risk to their organization.

Focus on Controls Rather Than Assets

The ways that security programs discuss reducing organizational risk typically focuses on the security controls and potential attacks, rather than on the purpose for that security measure. You can see this in how security professionals speak: "We have X technology to protect against Y attack."

Discussing organizational security this way focuses on the activity rather than the outcome. It's not "We're protecting our HR department from W2 fraud," instead the community often says "We have [control] to protect against phishing attacks."

> **Controls need to be Complete and Effective.**
>
> **Complete** - Control needs to exist in the places it's needed.
> **Effective** - The control actually reduces risk in the way the security program intended.

PART I

Misapplication of Frameworks and Compliance

The proliferation of frameworks, certifications, and compliance regimes have done enterprise information security a disservice. Many security teams spend significant resources maintaining processes that ensure they remain compliant with this requirement or show steady improvement in a framework.

Unfortunately, there's not a 1:1 relationship between compliance and security.

Compliance regimes can lead a security organization to orient towards maintaining compliance rather than reducing risk. The steady stream of media reports describing breaches of compliant organizations shows the ineffectiveness of these tools for security strategy.

The appeal of frameworks is that they mandate what an organization should implement, making it easier to build a plan and get buy-in. The downside is that frameworks mandate controls that may not make sense for a given organization. The lack of flexibility means organizations may be forced to invest in controls knowing they provide little benefit.

Organizational Inertia

Once security goals are decided, metrics agreed, and all briefed to management and the Board, it can be difficult to change them. The reality of cybersecurity is that risks can change quickly—shifts in technologies, attacker techniques, zero-days, international relations can all affect risk. Covid-19 provided a great example of how risk profiles can literally change over a weekend.

PART II

Principles of Effective Security Programs

If the above considerations can influence a security program away from effective activities, what are the common features of those security programs and leaders that are risk-informed and effective?

Risk is the Guiding Star

The purpose of the security organization is to reduce business risk. Security programs and efforts need to be directly and explicitly linked to risk—to why an activity will have a desirable outcome.

A Security Program Should Be Universal

An effective security program needs to provide an overarching strategy that guides the role of each specialization. Increasingly the application is the platform is the service is the network.

You Can't Boil the Ocean

Given resource constraints, focus controls first on those assets and processes that are most important to the business. Accept that "perfect" is the enemy of "good enough."

Compromise is Inevitable

A differentiator for effective programs is that they make similar efforts to develop, test, and improve capabilities to detect, respond, and recover as they make for validating protective controls.

PART II

Technical Verification and Rapid Evolution

Technical Verification is a Cornerstone

In any human-created system of sufficient complexity, there will be times that it does not operate the way its creators intended. If the purpose of a security organization is to reduce risk, it is vital that the program includes verification that controls work as intended.

Although most organizations have adopted penetration testing as a regular process, we still find that most organizations also have significant unknown technical risks in their environments.

> **Trust, but verify.** A verification program needs to expand beyond penetration testing to investigate the full suite of controls, including inventory verification, detective capabilities review, tabletop exercises, etc.

A Security Program Must Evolve Rapidly

The risk landscape changes due to circumstances outside an organization's control—new technologies, zero-days, media attention, pandemics, regional tensions. An organization's mission and focus can change rapidly, which then changes its place in the threat landscape.

> **A security program must be able to adapt at the same pace of changes to the organization's threat landscape, mission, and focus.**

PART III

The Hard Part: Implementation

We've established there is a problem and provided a very abstract description of how to solve it, but this is all just a thought exercise if nothing is actionable. This section provides an outline for implementing an adaptive, risk-informed security program.

Educate Your Management

If the principles described resonate with you but are not representative of your current security program, open a dialogue with senior leaders, executives, and the Board. The security program and related messaging may change dramatically from what they are used to seeing.

> **Biannual board briefings that show the same goals gradually move from orange to yellow to green are a thing of the past.**

Have Regular Self Evaluations of Risk

In order to identify the right things to efficiently manage risk, an organization needs to have an accurate understanding of its risk. Effective organizations will do this regularly, at least annually but as often as quarterly.

Verify Your Controls Work

For any technical control you implement, devise some form of "real world" testing to verify it works as intended. If you are lucky enough to have an internal red team, make sure they are heard. Ask them what keeps them up at night.

PART III

Practice, Practice, Practice

Similar to verifying that technical controls work, ensure that your processes (and people) can effectively execute those controls "after" prevention—Response, Restoration, and Recovery.

> **"Train like you fight; fight like you train."**

In times of high stress and limited time, an organization will rise or fall to the performance level of its practice. If you haven't practiced at all, it is unlikely that you will be successful. To run a high-performance security organization, take lessons from other high-performance teams in the military or professional sports, and set aside time to practice.

Foundational Security Controls

Based on the Verizon Data Breach Investigations Report, the top four actions related to breaches are Hacking, Social Engineering, Errors, and Malware. Our suggestions for foundational controls are based on preventing these classes of threats:

- **Patch and Vulnerability Management** - Mitigates vulnerability exploitation
- **Multi-factor Authentication** - Mitigates password compromise and theft
- **Application Whitelisting** - One of the most effective, far-reaching controls
- **Secure Configurations** - Device management to prevent errors
- **Endpoint Protection** - Protection against malware

CONCLUSION

Building an Effective Security Program

A core premise of this paper is that many organizations have ineffective security programs despite significant expenditures, and a major contributor is organizations spending time and money on the wrong things.

To get away from this, organizations should adopt and execute a regular process to evaluate their threat profile and security program, then calibrate controls based on the outcome—not just generic frameworks. Attempting to install a prescribed list of controls provided by a generic third party model is often going to lead to inefficiencies.

> **While many controls don't produce universal value, there are certain controls that are beneficial to every organization.** If implemented effectively, these controls can provide a strong foundation for a security program on their own.

Whether you are building a program from scratch or contemplating a refactor of an existing program, focus on the foundational controls as a starting point. Then, continuously evaluate, adapt, and evolve your program based on your organization's unique risk profile.

Ready to Build an Effective Security Program?

Partner with Praetorian to assess your security posture and implement risk-informed controls.

Contact Us

PRAETORIAN

www.praetorian.com | info@praetorian.com