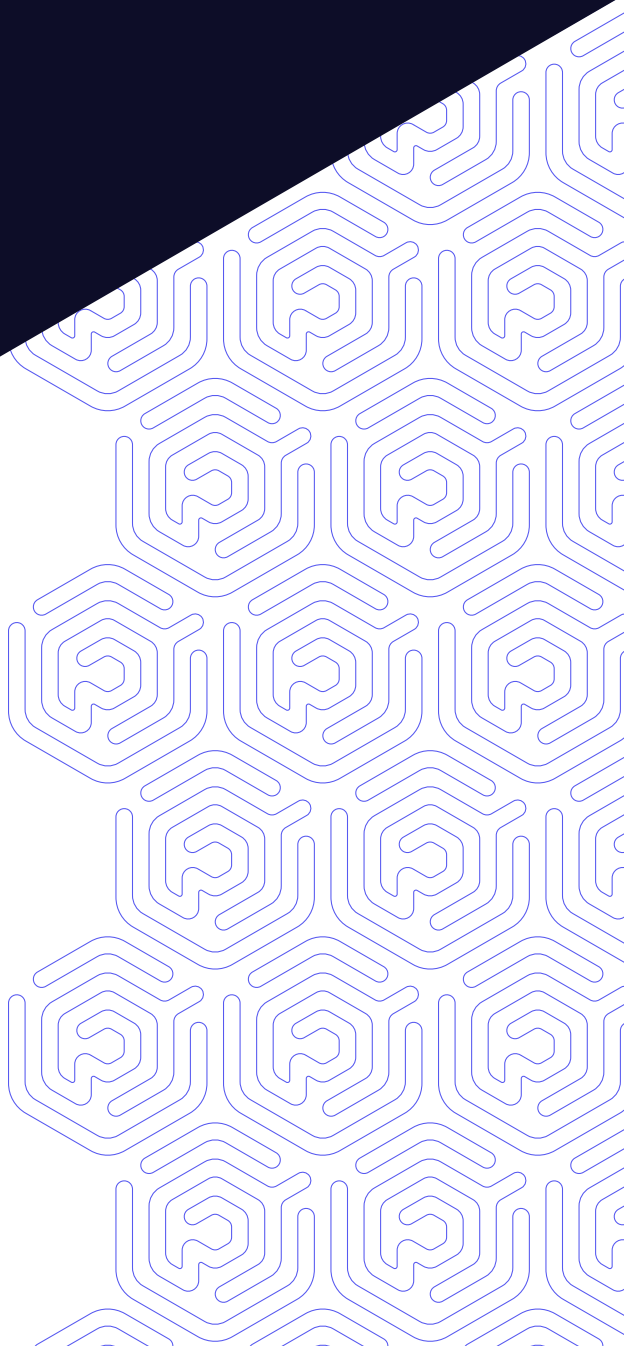
WHITE PAPER

The Elephant in the Room: Why Security Programs Fail



praetorian

Groundwork

The uncomfortable truth of the current state of cybersecurity is that 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 point to a sobering likelihood–better-resourced nation-states and criminal organizations are able to achieve similar results.

The troublesome state of cybersecurity in this regard is perplexing. Despite serious programs with smart people and millions of dollars invested, why do so many organizations still have significant gaps that we are able to find and exploit? Conversely, what are the common threads between those organizations that are able to keep us out, or find and evict us so quickly the result is the same?

> *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 things that do not appreciably reduce their organization's risk. Put differently, many organizations are engaged in activities that do not effectively improve their outcomes. Lots of effort, insufficient results.

A number of factors contribute to this, including but not limited to:

- **Relying on frameworks and compliance regimes to guide security programs, without sufficient attention to the organization's unique risks and threat profile (blind adoption)**

© Copyright 2021 Praetorian Group, Inc. All rights reserved. | praetorian.com

- Divergence of stagnant organizational priorities and metrics-tracking from ever-evolving risk
- Focusing on security controls rather than securing assets (performance vs. effectiveness)
- Failing to sufficiently verify that security controls were implemented properly and function as intended
- Stovepipes within the security organization, and between security and the rest of the business, such that the diffusion of roles and knowledge leads 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.

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. We hold these truths to be self-evident:

The Mission of a Security Program is to Reduce Organizational Risk.

A cybersecurity organization's mission is to reduce the likelihood of security incidents and reduce the costs (monetary or otherwise) associated with an incident should one occur. A security strategy and program need to keep that in front of mind. The mission isn't to keep an attacker from breaching the perimeter or prevent a DDoS attack of a core product; those are means to an end. Part of where many organizations go wrong is in confusing the core mission of the security program with its activities.

© Copyright 2021 Praetorian Group, Inc. All rights reserved. | praetorian.com

Words and Framing Matter

There's a philosophical underpinning to this paper that the words and thought patterns we use to define and describe a problem influence the solutions we develop for that problem. While the community largely accepts the mantra that cybersecurity is constantly evolving, many organizations use frameworks that are years old[1] in an unsuccessful attempt to grapple with a chaotic and messy reality. Cybersecurity as a discipline also largely grew out of the information technology department of most organizations, and many cybersecurity practitioners have engineering backgrounds. In many cases, we've brought the strategies and thought patterns from those disciplines into our cybersecurity programs[2] , without the introspection to notice that they often aren't efficient when applied to security and risk. Consequently, many organizations are thinking about and discussing cybersecurity in ways that are tangential to efficiently building a security program. Many discussions revolve around using technology to mitigate or prevent vulnerabilities, rather than focusing on risks and assets.

> *Many organizations are thinking about cybersecurity in ways that are tangential to efficiently building a cybersecurity program.*

An Effective Security Leader Identifies the "Right Things" for Focus

The "Right Things" are those activities that will reduce the organization's risk most efficiently. Put differently, what activity will reduce the most organizational risk if provided additional headcount, time, or money? The challenge is that there will always be multiple right things, and they will shift over time. This shift can be due to diminishing returns from investing in any one thing or due to changes in the risk and threat landscape.

1 ISO 27001 - 2013, NIST CSF - 2014, SOC 2 - 2010, PCI DSS - 2004
2 This is a similar idea to Conway's Law: "Any organization that designs a system (defined broadly) will produce a design structure is a copy of the organization's communication structure." https://en.wikipedia.org/wiki/Conway%27s_law

© Copyright 2021 Praetorian Group, Inc. All rights reserved. | praetorian.com

If the goal of a security program is to reduce organizational risk, then a mark of an effective security leader is being able to identify the right things for their security organization. Risk can never be reduced to zero, but a security leader can help ensure that the organization uses its security budget for maximum effectiveness in reducing risks. Effective leaders are able to balance shifts in risk, evaluate new solutions, identify diminishing returns, avoid sunk cost fallacy, etc. to ensure that their organization's[1] activities are most efficient.

Structure

This paper consists of three parts. It is intended to help those responsible for setting security strategy understand the common root causes of security programs' strategic failure and take steps to evolve to a more effective, risk-informed program.

- **The factors that cause many security programs to misdirect their time and efforts away from the things that would help them the most**
- **The common elements of a risk-informed, effective security program**
- **Foundational steps for implementing a risk-informed security program**

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

© Copyright 2021 Praetorian Group, Inc. All rights reserved. | praetorian.com

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 to secure the enterprise 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. In many cases, as an outsider looking in, we can see that they have focused on the wrong things.

A few themes emerge for how this happens. They are detailed below.

Focus on Security Controls Rather than Securing 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 at tax season," instead the community often says "We have <control> to protect against phishing attacks."

Our theory is that this comes from cybersecurity's evolution largely out of information technology and engineering. Many cybersecurity professionals came from IT and engineering backgrounds, and they brought with them the attendant philosophies and thought patterns.

© Copyright 2021 Praetorian Group, Inc. All rights reserved. | praetorian.com

These include identifying technologies that solve the organization's problems. Neither IT nor engineering typically is called on to define their organization's problems, but instead to provide a solution for them.

Conceptualizing and discussing security controls as solutions for vulnerabilities can lead to misspent time and effort. Any given control doesn't matter unless it's matched to reducing a business risk. Discussing the actions of a security program as controls rather than in terms of risk reduction divorces them from their purpose and creates inefficiencies.

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

Ultimately, an attacker's ability to breach an environment is dependent on at least one of these two traits being absent in an environment, and the reality is that they are missing in many organizations. A legacy portal lacking multi-factor authentication (MFA), misconfigured endpoint protection, etc. can all represent a single gap that results in the failure of a security program.

When evaluating your security controls and program, it is key to keep these two traits in mind. Faulty assumptions or ineffective auditing and/or verification create situations in which an organization wrongly believes these questions to be true.

- **Are your controls enacted everywhere that they need to be?**
- **Have you verified that each control is effective?**

These concepts are central to an effective security program and will repeat in different ways throughout this paper.

© Copyright 2021 Praetorian Group, Inc. All rights reserved. | praetorian.com

Misapplication of Frameworks and the Distraction of Compliance

The proliferation of frameworks, certifications, and compliance regimes have done enterprise information security a disservice. Many security teams spend significant resources maintaining the processes that ensure they remain compliant with this requirement or show a steady trend of improvement in a framework. Unfortunately, there's not a 1:1 relationship between compliance and security, and they can lead a security organization to orient towards maintaining compliance rather than reducing risk. We believe that the steady stream of media reports describing breaches of enterprise organizations, most of which are compliant with one or more frameworks, shows the ineffectiveness of these tools for security strategy and governance.

> *The proliferation of frameworks, certifications, and compliance regimes have done enterprise information security a disservice.*

The appeal of frameworks and compliance regimes is that they mandate what an organization should implement. Frameworks make it easier to build a plan, and a framework can provide credibility when getting buy-in for that plan from stakeholders. It's tempting to build a security program around a list of things a reputable organization has provided. You simply go implement them and measure your progress, right?

The downside of this approach is that these frameworks and regimes will mandate security controls that may not make sense for a given organization. The lack of flexibility in compliance regimes also means that organizations may be forced to invest in certain security controls, knowing that those controls will provide little benefit in reducing the organization's actual risk.

Security Maturity Models were offered as a solution to these problems. Rather than providing an inflexible list of controls to be implemented,

© Copyright 2021 Praetorian Group, Inc. All rights reserved. | praetorian.com

maturity models allow organizations to choose an appropriate set of security controls or objectives based on the organization's unique considerations. While we think this approach is an improvement over a compliance approach, in our experience, maturity models typically lead to similar problems. A maturity target is still a step removed from actual organizational risk. Human nature often leads to an arbitrary selection of a higher maturity target state, rather than calibrating the target based on unique organizational risk. Then, once a maturity target is chosen, meeting that target becomes the goal, rather than activities that will directly reduce risk.

Organizational Inertia

The realities of how businesses operate can also redirect security efforts towards efforts that are not optimal for reducing risk. Once security goals have been decided, metrics agreed, and all briefed to management and the Board, it can be difficult to change them for personal and political reasons. Understandably, most security practitioners would rather brief management on steady improvement or maintenance of their metrics. It would be uncomfortable to explain to most boards that something the CISO briefed as absolutely the most important last year now isn't even in the Top 3 this year. Some organizations will also tie individual performance and incentive compensation to these metrics, which can make practitioners within the security organization especially reluctant to change those metrics, even if they become less relevant.

The reality of cybersecurity, though, is that risks can change quickly, and in shorter timeframes than most business cycles. Shifts in technologies, attacker techniques, zero-days, international relations, etc. can all affect an organization's risks. Covid-19 and the rapid adoption of work from home provide a great example of how an organization's risk profile can literally change over a weekend.

If at the end of the annual cycle, an organization doesn't feel that it needs to update any of its security goals or metrics, you should take a second look and question its underlying assumptions. If at the end of two years you do not feel that you need to update objectives and metrics, you are probably doing something wrong. Organizational inertia can provide powerful incentives, however, for keeping those metrics unchanged.

© Copyright 2021 Praetorian Group, Inc. All rights reserved. | praetorian.com

Part II: Principles

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? The below are principles that we have identified as contributing to adaptive and typically more effective security programs.

Risk is the Guiding Star of the Security Program

The purpose of the security organization is to reduce business risk. Security programs and the efforts they undertake need to be directly and explicitly linked to risk, to why an activity will have a desirable outcome. Start with Why. Too often security initiatives are not explicitly linked to their goal in terms of risks. When this linkage isn't explicit, there is a tendency for inefficiencies to creep into security activities. People start doing things based on fear, uncertainty, and doubt rather than as part of a conscious strategy to reduce risk. This leads to security investment spent on activities orthogonal to the actual goal and spends that do not appreciably help the organization.

A Security Program Should Be Universal

Within the realm of cybersecurity, there have developed a large number of specializations and niches. You can see on Twitter and through conferences and job postings how the cybersecurity community divides itself into red team, blue team, defenders, offensive security, product security, cloud security, etc. An effective security program needs to be universal, and provide an overarching strategy that guides the role of each of these specialties.

This is particularly important as we see infrastructure and applications start to converge. Increasingly the application is the platform is the

© Copyright 2021 Praetorian Group, Inc. All rights reserved. | praetorian.com

service is the network. A security program that thinks of each of these separately is going to create underlaps and overlaps in how an organization reduces its risk. Instead, starting from a perspective of risk rather than technology, a security program needs to provide a universal strategy that guides the role these individual disciplines play.

You Can't Boil the Ocean

An organization has a finite amount of time, money, and mental energy. Given resource constraints, focus controls first on those assets and processes that are most important to the business. If a program orients from the perspective of technical controls, it's too easy to get bogged down in layering technical solutions without consideration for their reduction in risk. Orient from the perspective of business risk instead of technical risk, and focus efforts from there. It's perfectly fine to accept that some security controls may not be perfect or cover the whole organization as long as the critical assets and resources are covered.

There are also often diminishing returns when implementing security controls. There's often a point where an increase in effort leads to less and less outcome in terms of effectiveness and reduced risk. Accept that "perfect" is the enemy of "good enough," and be explicit with your strategy that "good enough" is… good enough.

Compromise is Inevitable

The idea that compromise is inevitable has permeated the security community as a universal truth, but many organizations' security programs still do not reflect it in practice. In many organizations, the effort paid to detection, response, and recovery is anemic relative to the effort spent on protective controls and compliance.

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

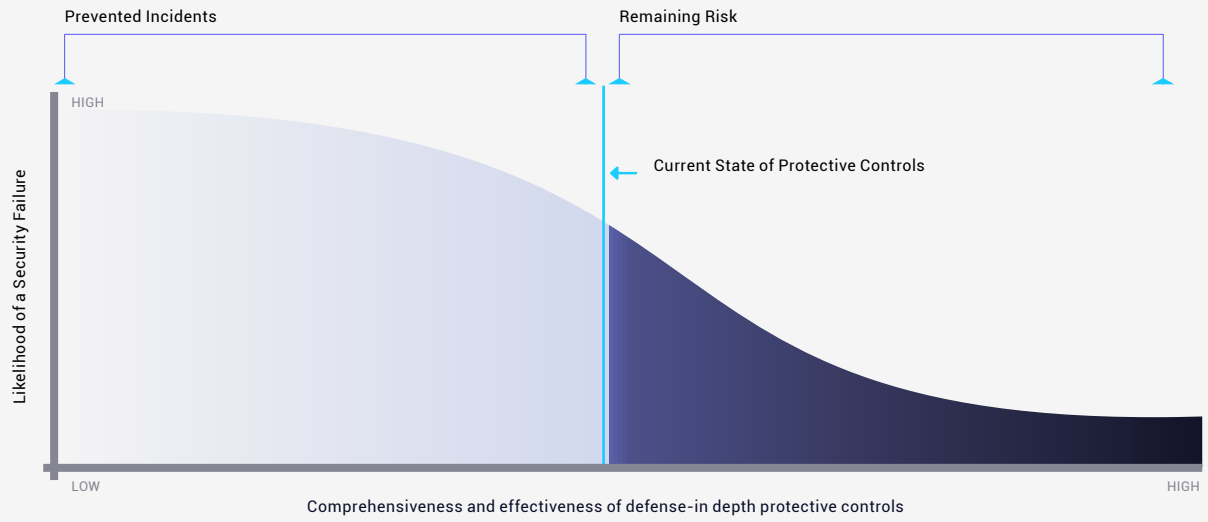
© Copyright 2021 Praetorian Group, Inc. All rights reserved. | praetorian.com

Protective Technical Controls Reduce the Risk/Frequency or Incidents to Manageable Levels.

Related to the previous two points, pragmatic security programs will accept that they can't be perfect all the time and 100% prevention of incidents is not a realistic goal. Instead, their strategy will acknowledge that incidents are inevitable, and it's not cost effective to seek to prevent them entirely.

Instead, an effective security program will seek to find the sweet spot of where the diminishing returns of investing in protective controls mean investment would be better spent on improving detection, response, and recovery capabilities. The goal is to ensure that protective controls keep the actual occurrence of security incidents below the level that the security team is able to detect, contain, and recover.

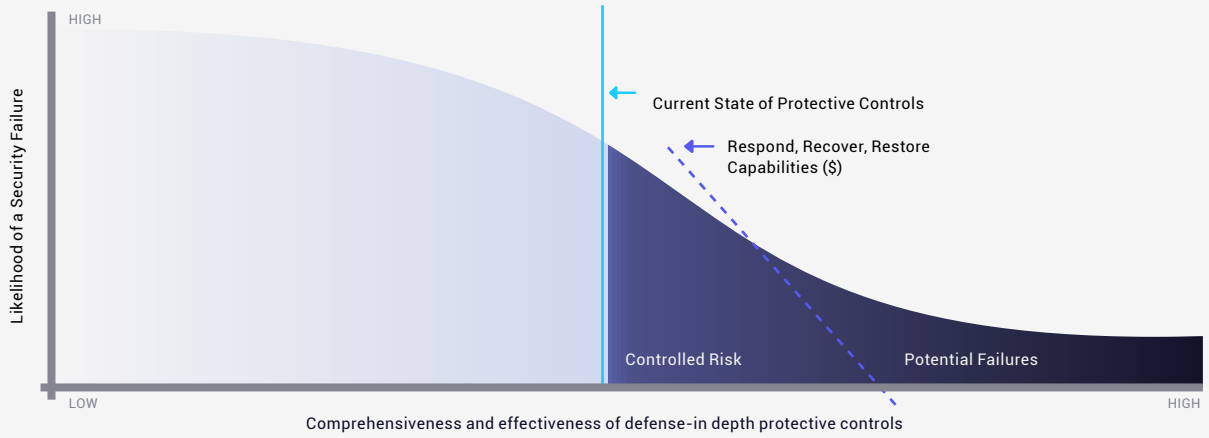
The Economics of Security Effectiveness



© Copyright 2021 Praetorian Group, Inc. All rights reserved. | praetorian.com

The curve represents how the likelihood of a security failure (i.e. an incident) decreases as the comprehensiveness and effectiveness of protective controls increase. You can generally move your current state to the right through additional resources; however, this relationship has diminishing returns and there is a point at which each dollar spent has less and less impact in reducing risk.

Wherever an organization sits along this curve, they will have risk remaining, due to gaps in their protective controls. They can mitigate this risk by increasing their capabilities to detect, respond, and recover from an incident, which reduces the probability of a security failure (i.e. a breach). See the graph below.



There's a delicate balance in an effective security program of trying to understand when a given dollar would have a greater reduction in security failures by either moving farther along the curve or increasing the capability to detect, respond, and recover from an incident. The goal is always to reduce the realm of potential security failures. The difficulty of this proposition is compounded, however, by the fact that these lines are constantly shifting and an organization rarely knows where either of the two lines is at any point in time.

The science and art of being an effective security leader is to make (accurate) educated guesses about where these lines are at any given time, and then allocate their organizational resources to minimize the area of potential failures/uncontrolled risk.

© Copyright 2021 Praetorian Group, Inc. All rights reserved. | praetorian.com

Technical Verification is a Cornerstone of an Effective Security Program

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

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 and assets

> *There will be times that any system doesn't operate the way its creators intended.*

Part of this is due to the inherent limitations of most penetration tests. Whereas persistent attackers do not have constraints on their time or techniques, penetration tests are constrained in order to limit costs. They are time-boxed; the scope is provided by the organization being tested; they typically disregard stealth and evasion techniques; they focus on most likely attack paths rather than most dangerous, etc. Penetration testing also focuses on protective controls, so a mature pen testing effort alone will not kick the tires of inventory practices, governance, detection, response, recovery, etc. We often discover security gaps that our clients could easily have found themselves, but it was simply the case that no one ever thought to look[3].

If a security program relies on a control to reduce risk, it is important that some kind of validation occurs to ensure that the control is **effective**. We'd further suggest that the validation needs to be performed with a method that verifies that the control actually works in real-world conditions. Audits that use interviews and policy review alone cannot

3 While this is based on my anecdotal experiences, we see this most often in detection controls. We find that many organizations dramatically overestimate their ability to detect, and then respond to an attack. We often find significant gaps in visibility and processes when these controls are tested against a sophisticated attack.

© Copyright 2021 Praetorian Group, Inc. All rights reserved. | praetorian.com

be relied on for accuracy. Human error is inevitable, and what people think is true is often wrong. Trust, but verify. A verification program also needs to expand beyond penetration testing to investigate the full suite of controls, including things like inventory verification, detective capabilities review, tabletop exercises of response plans, etc.

A Security Program Must be Capable of Evolving Rapidly

As previously mentioned, the risk landscape changes due to circumstances outside an organization's control. New technologies, zero-days, media attention, pandemics, regional tensions, etc. can all affect an organization's risk. Likewise, an organization's mission and focus can change rapidly, which then changes its place in the threat

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

landscape. A security program must be able to adapt at the same pace. Almost no market or organization is static, so a security program that is protecting what was important last year is almost certainly inefficient, and spending some portion of its time and money in less impactful ways.

An effective security program operates in close collaboration with other business units to anticipate these changes and adapt to them as needed. Leadership understands that metrics and OKRs are abstractions of a reduction in risk. If the sources for risk change, risk needs to guide the security organization's efforts rather than those metrics.

© Copyright 2021 Praetorian Group, Inc. All rights reserved. | praetorian.com

Part III: The Hard Part

We've established there is a problem and provided a very abstract description of how to solve that problem, but this is all just a thought exercise if nothing is actionable. The purpose of this final section is to provide an outline for implementing an adaptive, risk-informed security program. The first part describes what each of the principles can look like in action. The second section describes a small set of foundational security controls recommended for every organization.

It's not lost on the author that the second section somewhat violates the premise of this whole paper - that the relative importance of security controls will vary between organizations. These particular controls are suggested based on how they address nearly universal risks. The section also includes an explanation of why they are suggested, so that you can evaluate their utility for yourself. While not all controls are as important to all companies, the suggested controls will be powerful for

> *While many controls don't produce universal value, there are certain controls that are beneficial to every organization.*

any 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, these would be the controls we suggest as a starting point.

Strategic Practices in Action

The practices described here are really restating the principles as the opposite side of their coin. These are intended to provide a high-level description of what that principle looks like when implemented by a CISO and/or security program.

© Copyright 2021 Praetorian Group, Inc. All rights reserved. | praetorian.com

Educate your Management

If the principles described above resonate with you but are not representative of your current security program, we suggest opening a dialogue with senior leaders, executives, and the Board to prepare them for changes in the security program. The security program itself, and the related messaging to management, may change dramatically from what they are used to seeing. One of the first steps for transitioning to a more adaptive, risk-informed program is to get senior leadership's buy-in.

Praetorian suggests sharing many of the themes contained here. Prepare them that risks change, often rapidly. Your security program is going to evolve and may not look like what they are used to. Biannual briefings that show the same goals gradually move from orange to yellow to green are a thing of the past. Explain why that is a good thing, that it means you're evolving apace with the threat. Your security organization is becoming agile and adaptive. You may tell them something totally different from one quarter from another.
Reassure your senior leadership that it is completely fair for them to challenge you on these changes, both now and in the future. Part of their job is to understand the organizational risk and provide oversight that the security program is managing it effectively. They should be involved in the process of ensuring that the security program is focused on the right things, at any given time.

> *Biannual board briefings...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. We think the most effective way to do this is similar

© Copyright 2021 Praetorian Group, Inc. All rights reserved. | praetorian.com

to threat modeling but at the organizational level. Break the organization down into business objectives and subcomponents, identify the critical components and processes, and enumerate the threats to those crown jewels. Once the threats are identified, risk can be evaluated and a strategic plan developed.

For this process to be effective, nothing should be sacred or unquestionable. Try to acknowledge your assumptions and question them. Identify what has changed since the last such exercise in terms of your business, technologies, architecture, international relations, etc. and ask how those changes might affect your risk. Do you need to reprioritize because of it? Is there anything that can be deprioritized because of these changes? Have you noticed that you're getting diminishing returns from an activity you're already doing? Are you seeing an increase in a certain kind of attack against yourself or similar organizations?

This process then informs the security strategy and the path toward identifying the right things to most efficiently reduce risk. Based on the insights from the exercise, evaluate what activities you can increase, sustain, or decrease. Again, don't seek to boil the ocean and institute perfect security measures everywhere. Instead, focus on instituting perfect controls where they are truly needed and making other decisions based on risk.

Verify Your Controls Work

For any technical control, you implement, devise some form of "real world" testing to verify that it works as intended, across intended cases. Many organizations are used to working with third-party or internal penetration testing/red teams. Those efforts are great, but control verification should be more expansive than what is typically considered penetration testing. Figure out ways to verify that your inventories are both accurate and comprehensive. Verify that if malware is launched on a workstation that it is blocked, an alert is generated, and a process kicked off to quarantine and respond. Try to make the conditions for all of this testing as realistic as possible, minimizing restraints that wouldn't affect a true attacker.

© Copyright 2021 Praetorian Group, Inc. All rights reserved. | praetorian.com

As a side note, working with many organizations, we hear a common theme in which internal red teams have warned about security gaps and been ignored. If you are lucky enough to have an internal red team, make sure that they are heard. Ask them what keeps them up at night, and be prepared to listen, no matter how uncomfortable that conversation may be.

As you identify places where controls fail and dig into root causes you may find places where organizational design contributes to or outright causes the failure. Be aware that your toolbox for addressing a problem may require changes to teams and responsibilities. Sometimes a change in organizational design will be the most direct way to ensure that your defenders have the information and easy access to colleagues required to respond to an incident quickly and effectively.

Practice, Practice, Practice

Finally, similar to verifying that your technical controls work, ensure that your processes (and people) can effectively execute those controls "after" prevention - Response, Restoration, and Recovery. There's a maxim in the military "Train like you fight; fight like you train," summarizing the concept that 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. Similarly, if you haven't practiced enough for stakeholders to know their roles and how to perform their responsibilities, or if you've practiced under unrealistic conditions, those iterations will provide limited help in an actual incident.

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

In contrast, if your team has responded to similar events multiple times in training exercises, they're likely to perform well at the time of a true incident. No one will waste time digging through Sharepoint to find an outdated playbook with its phone tree in order to know who to call in

© Copyright 2021 Praetorian Group, Inc. All rights reserved. | praetorian.com

Legal. Kinks and pitfalls in the process can be identified and worked out through training. Team members get iterations using tools and processes and can react faster because of it.

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.

Tactical

A core premise of this paper is that many organizations have ineffective security programs despite significant expenditures and that a major contributor to this is organizations spending time and money on the wrong things. In turn, one of the causes for that are frameworks and compliance regimes that force the implementation of some controls despite the fact that the relative importance of any specific security control will vary for each organization and over time. To get away from this, organizations should adopt and execute a regular process to evaluate your threat profile and security program, and then calibrate controls based on the outcome of the evaluation, not just generic frameworks. Put differently, attempting to install a prescribed list of controls provided by a generic third party model is often going to lead to inefficiencies.

We would be remiss were we to suggest that each organization has to ignore common frameworks and build their own unique security program from the ground up. There do exist a set of controls that provide an effective foundation for any organization's security program. The challenge is finding the balance between common controls that all organizations benefit from, and controls that only certain organizations benefit from.

This list is informed by the Verizon 2020 Data Breach Investigations Report (DBIR). As of the 2020 report, the top four actions related to breaches and incidents were Hacking, Social Engineering, Errors, and Malware. These four activities represent most of the baseline "white noise" in the threat landscape and are threats that almost all organizations can reasonably expect to experience at some point.

© Copyright 2021 Praetorian Group, Inc. All rights reserved. | praetorian.com

Our anecdotal experience from an adversary perspective matches the DBIR's findings. Those four classes are also our most common way to breach a network perimeter during red team exercises mimicking an APT actor. Praetorian's suggestions for foundational controls are based on preventing these classes of threats.

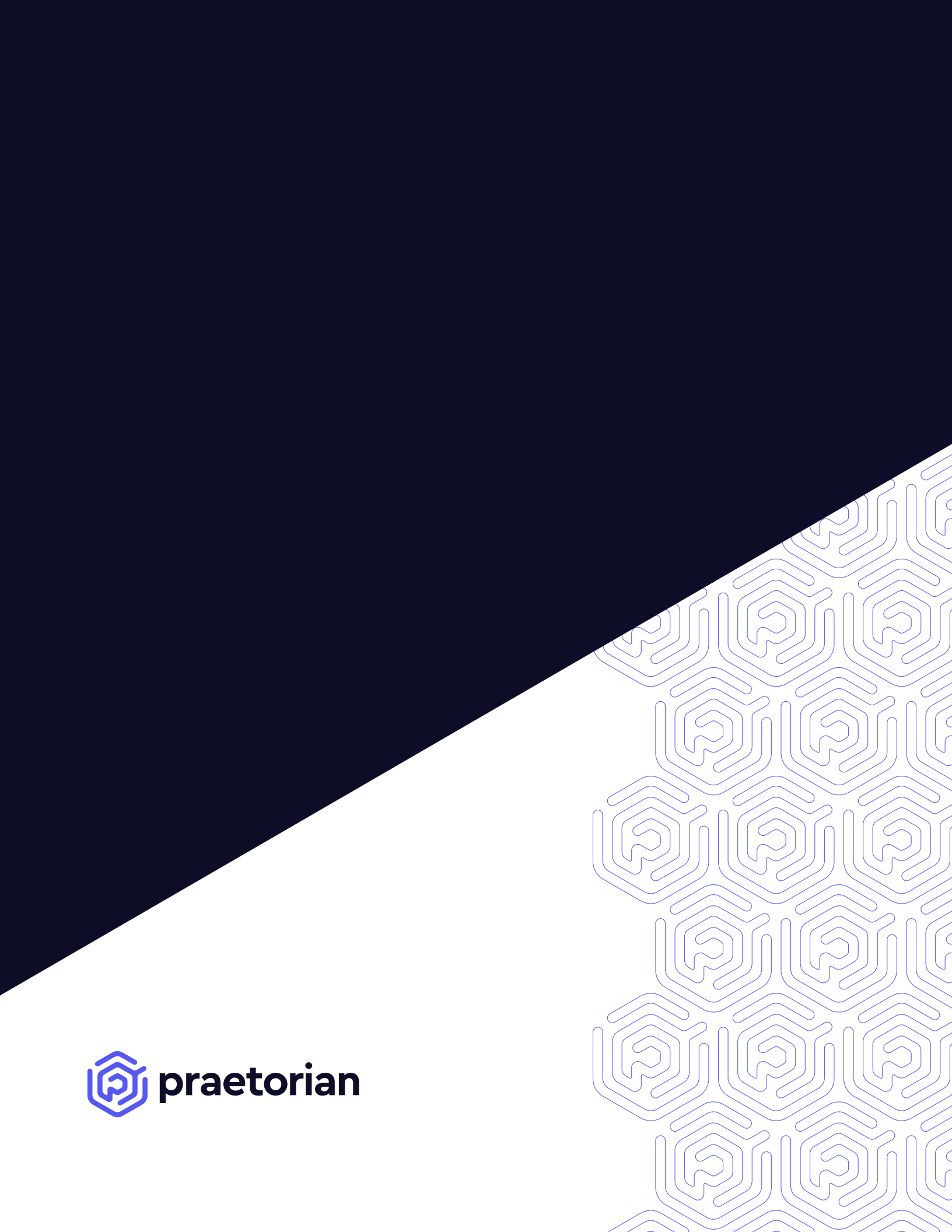
The below table identifies the five controls that will protect an organization from the most common type of attacker activities. Implementing these controls through an organization and verifying that they are effective would yield a strong foundation for any security program. Additional controls can then be implemented and tailored based on the unique considerations of the organization.

THREAT	MITIGATING CONTROL
Hacking	Patch and Vulnerability Management (mitigates vulnerability exploitation) Multi-factor Authentication (mitigates password compromise) Application whitelisting (mitigates vulnerability exploitation)
Social Engineering	Multi-factor Authentication (protects against password theft) Application whitelisting (protects against malware)*
Errors	Secure configurations and device management
Malware	Application whitelisting (protects against malware) Endpoint protection

A Word on Application Whitelisting

Application whitelisting is one of the single most effective, far-reaching controls you can implement. That said, many rightfully point out that it's hard to implement. While true, it is often a lower effort (and much lower cost) than implementing all the other technical controls used in place of app whitelisting. Further, app whitelisting tends to be more complete and effective than the hodgepodge of controls implemented to achieve the same goal.

© Copyright 2021 Praetorian Group, Inc. All rights reserved. | praetorian.com


praetorian