THREAT AND VULNERABILITY MANAGEMENT

THE ROLE OF THREAT MODELING IN A MODERN CYBERSECURITY OPERATIONS PROGRAM

COALFIRE LABS

COALFIRE®

North America | Europe
877.224.8077 | info@coalfire.com | coalfire.com

TABLE OF CONTENTS

CYBERSECURITY IS HARD

Careful planning and discipline are required to build an appropriate cybersecurity program for an organization. The IT landscape is continually evolving, driving the constant evolution of security toolsets. Selecting the appropriate technologies and operational models for your organization can be a complex decison—there's a technology available for every security situation imaginable. This is further compounded by the unfortunate reality that a CISO often inherits many tools and processes from their predecessor which may or may not be optimized for the business or comprehensively deployed. Finally, many of these organizations have implemented technologies and processes and even "best practices" without considering strategic alignment with business priorities. They are following the "prudent man" model—doing what appears to be recommended in the industry, but without direct regard for the security objectives that drive the business.

Measuring value is hard

Building a modern cybersecurity operations team requires significant investment. Cyber operations budgets can become quite large, even for simply maintaining the status quo and accounting for only the minimum viable technology, staff, and training. New initiatives are even harder to justify. Conceptually speaking, ROI or other traditional IT measurement factors have too much subjective wiggle room to support actual quantitative calculation for security initiatives. Accordingly, how does one present the value of an investment into preventing an event that doesn't happen? Unless that organization has had the misfortune of being subject to a wide variety of failures, it's all really just guesswork.

Measuring success is hard

Along with being able to justify the investment, a cybersecurity program will need to be evaluated for effectiveness on an ongoing basis. Measuring "success" in a cybersecurity operations program is a problem for evaluating even the simplest technology investment, let alone the investment into people and processes. Traditional maturity models can be used to address this, but ultimately, they are part of the "prudent man" model as well, where "maturity" is a term relative to the program. They can measure the extent of deployment of the practice and technology set but fall short of identifying whether the program is meeting the objectives of the business. To their credit, maturity models have the distinct upside of being able to measure how complete a cybersecurity practice is at a given point in time. And while this is obviously quite beneficial, it does nothing to measure whether that practice is operating in alignment with the priorities of the business.

How can a CISO compete?

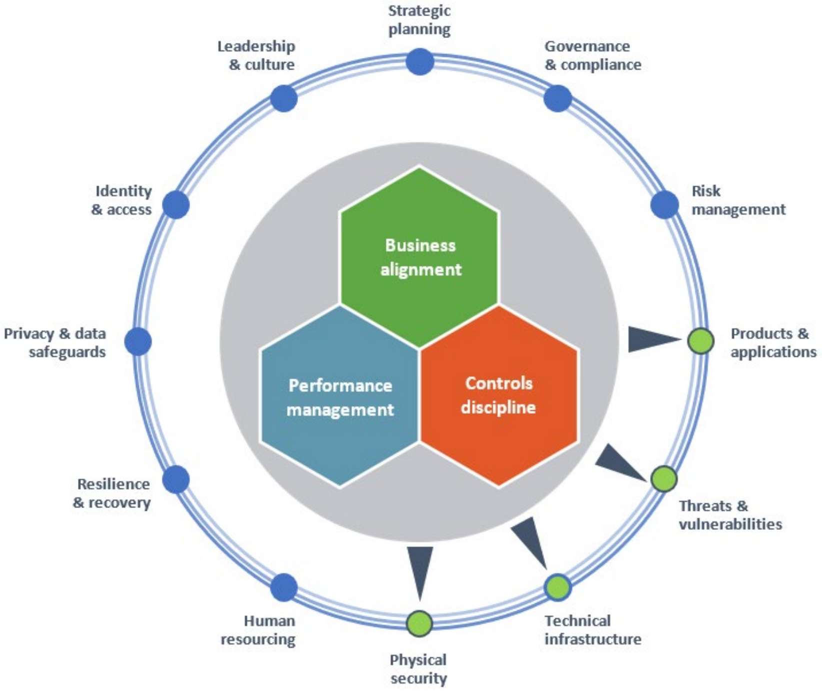
When competing for budget allocation with other business priorities, CISOs often struggle to demonstrate the value of investments that will support their cybersecurity program. The competition they're up against is internal, where other departments across the organization can justify their budgets using traditional models like ROI, revenue generation, profitability, or pipeline build through opening new markets. A CISO comes up short as those models rarely make sense in a typical enterprise security program.

- How does one determine which gaps are the most important for the business to address?
- How does one determine that there is a real need for a security solution rather than falling prey to the "cool factor" of a popular solution?
- How can one tell that an existing security control or process has outlived its usefulness?

The answer to these questions is to do it by going back to the basics. A tactical problem merits a tactical solution.

HOLISTIC CYBERSECURITY PROGRAMS

Coalfire has developed a framework called **Strategy+** that provides an excellent reference from which such determinations can be made. The framework is actually a three-dimensional model that provides guidance for 12 key domains in a cybersecurity program.



Coalfire's definition of a holistic cybersecurity program addresses all 12 domains, one of which is Threat and Vulnerability Management. Most organizations have a few components of *Vulnerability Management* in place already, usually vulnerability assessment, patch management, and penetration testing. These serve as a performance management check of security technologies and processes deployed within the organization. It's a good start at ensuring risk is kept to a minimum. However, many organizations haven't quite developed the *Threat* part of the Threat and Vulnerability Management program. Far too often, threats are overlooked, yet they are key to the process of risk assessment.

Threat identification for dummies

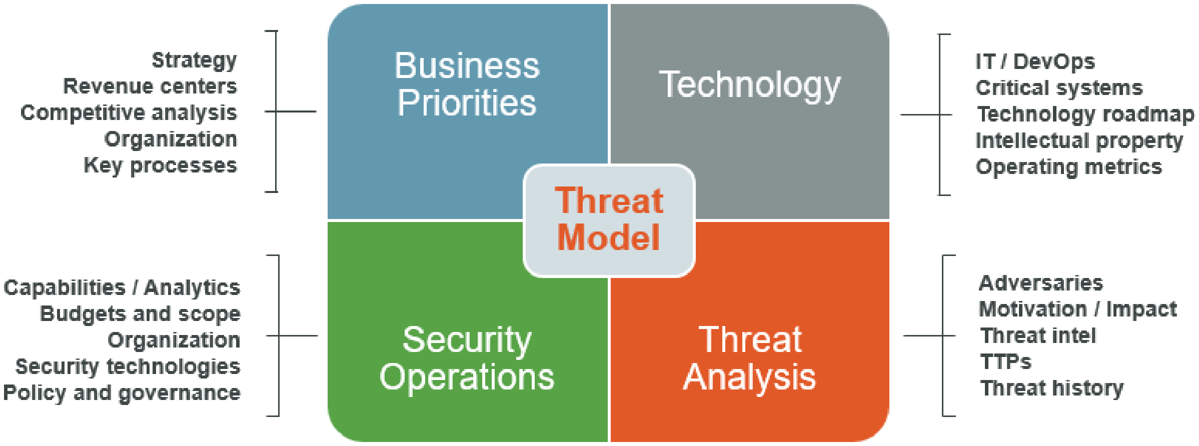
For the purpose of this paper, the term threat has a multi-faceted definition. Threats consist of actors and vectors. Threat actors are either a person or a situation. Threat vectors are methods by which an actor might attack. A credible threat is an actor that can align itself to vectors that are effective at impacting your business. Typically, that impact could be gaining access to an asset, compromising a process or company reputation, or bringing operations to a halt. Threats align with your business—your security program should too. By building a security program that aligns with threats to the business, you are also aligning your cybersecurity program to the priorities of the business.

Threat modeling

Threat modeling is a process for capturing, organizing, and analyzing all of the information that affects a system and assembling it into a structured representation of its security posture. When (traditionally) applied to an application or discrete system, the assets and processes that manage them ultimately define themselves. These are almost always comprised of data and the code library that handles the data. When applying this to a business, however, identifying assets can be the most challenging part.

Threat modeling starts by identifying the organizational assets to be protected based on the mission of the business. Understanding the unique value that the company provides to its customers and how that value is delivered through technology drives the identification and prioritization of assets. For many companies, prioritization is generally tied to short- and long-term sources of revenue or profit, thereby providing a direct correlation between the technical resource and the business objectives.

With this list of technical resources prioritized against business objectives now assembled, the next step is to identify any threat actors that would have motive and means to disrupt the business mission. Many organizations face a common group of threats as a consequence of merely being in business and connected to the internet. However, as businesses are unique and differentiated even among competitors in the same industry, there will inevitably also be a unique set of threat actors each company faces. Looking at historical security events within the organization and within the industry, and then augmenting this with threat intelligence sources from the cybersecurity community, will provide a company with the visibility into their most likely adversaries.



Measuring value

Building a testing capability that includes threat modeling into your threat and vulnerability management program ensures that testing activities can demonstrate the effectiveness of your security program in defending the business. Moreover, it can help steer the program while weeding out other programs that waste resources defending against a threat that isn't applicable to the business. Now that the assets are prioritized and threat actors have been identified, you can assemble credible testing scenarios to demonstrate the need—or lack thereof—for specific security investments. The MITRE Corporation, a U.S.-based non-profit federally funded research facility has produced their ATT&CK Framework, which can be used to lay out attack paths that include techniques specific to a security investment.

For example, suppose an organization is considering an investment into migrating endpoint detection and response technologies from one solution to another due to the new solution’s capability to detect dynamic library hijacking on Mac platforms. Using the threat model, that organization could first determine if that is indeed a credible threat, based on the identified threat actors and the impact to assets an attacker could achieve. Subsequently, the company could include this technique in an attack path that mimics the adversary’s attempts to compromise the asset. If the test demonstrates that this persistence/escalation technique can be executed without any existing analytics or detection capability, the justification for this investment can be traced directly to the value of the asset that supports the company’s mission.

This takes your threat and vulnerability management program to the proverbial “next level” on the maturity model scale.

Measuring success

The **Strategy+** framework is three-dimensional and is positioned to be leveraged as a maturity model for an organization’s cybersecurity program. The three dimensions are business alignment, performance management and controls discipline, and they help answer three fundamental questions every cybersecurity professional asks:

- Business Alignment: How does my security program benefit the business?
- Performance Management: How do we know it’s working?
- Controls Discipline: Are we doing the right things?

By implementing threat modeling and attack simulation into your cybersecurity testing processes, you are ensuring alignment with business objectives and ensuring the right investments are being made for the right reasons.

CONCLUSION

Measuring the value and success of any cybersecurity program is difficult, because ROI and other common KPIs are simply not applicable in the world of cybersecurity. Every CISO is competing for investment dollars on that uneven playing field, trying to justify necessary capital expenditures that don't necessarily sell themselves.

However, a holistic approach to threat and vulnerability management is possible. Coalfire's **Strategy+** framework ensures that your security measures and tactics align with your organization's business objectives. Our threat modeling and attack simulation services move your security posture to the next level of protection.

While it is tempting to default to the "prudent man" model when evaluating your company's current and future cybersecurity program, it's important to remember that there are more robust models available that effectively tie cybersecurity to business objectives to create a holistic threat and vulnerability management program that truly protects your business assets.

ABOUT COALFIRE LABS

Coalfire Labs applies knowledge gained from industry-recognized research of vulnerabilities, development of tools and exploits, and previous technical testing experience and then employing them in client testing engagements like an adversary would. This provides clients the simulated experience of an adversarial attack against their product or their business with an outcome that enables clients to remediate vulnerabilities, strengthen security posture and reduce risk (of the corporate crown jewels being compromised).

The Coalfire Labs team are highly skilled security professionals that use best-of-breed technical security assessment methodologies and unmatched analysis capabilities to help you fully understand the effectiveness of your organization's security operation.

ABOUT COALFIRE

Coalfire is the trusted cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for nearly 20 years and has offices throughout the United States and Europe. For more information, visit. **Coalfire.com**

Coalfire is solely responsible for the contents of this document as of the date of publication. The contents of this document are subject to change at any time based on revisions to the applicable regulations and standards (HIPAA, PCI DSS, et. al). Consequently, any forward-looking statements are not predictions and are subject to change without notice. While Coalfire has endeavored to ensure that the information contained in this document has been obtained from reliable sources, there may be regulatory, compliance, or other reasons that prevent us from doing so. Consequently, Coalfire is not responsible for any errors or omissions, or for the results obtained from the use of this information. Coalfire reserves the right to revise any or all of this document to reflect an accurate representation of the content relative to the current technology landscape. In order to maintain contextual accuracy of this document, all references to this document must explicitly reference the entirety of the document inclusive of the title and publication date; neither party will publish a press release referring to the other party or excerpting highlights from the document without prior written approval of the other party. If you have questions with regard to any legal or compliance matters referenced herein, you should consult legal counsel, your security advisor, and/or your relevant standard authority.

WP_Threat and Vulnerability Management_06162020