CYCOGNITO

EXECUTIVE BRIEF

ADVICE TO A NEW CISO

Build Credibility by Taking Stock Quickly and Effectively

Whether you are new to the role of chief information security officer (CISO) or just new to this particular organization, as CISO you have a unique opportunity to demonstrate your leadership in this critical position. This document, *Advice to a New CISO*, is designed to help you get out of the gate effectively and efficiently with new approaches that leading-edge CISOs are beginning to implement. In just three pages, we'll cover:

01 Begin with Attack Surface Management as Your Security Program Foundation One of your first priorities as a CISO should be to assess your organization's risks so you can effectively allocate and prioritize your security program resources. Based on the most common tactics attackers use to breach your organization[1], there are two broad areas of risk exposure you need to consider. These are your:

- Attack surface
- Users and endpoints

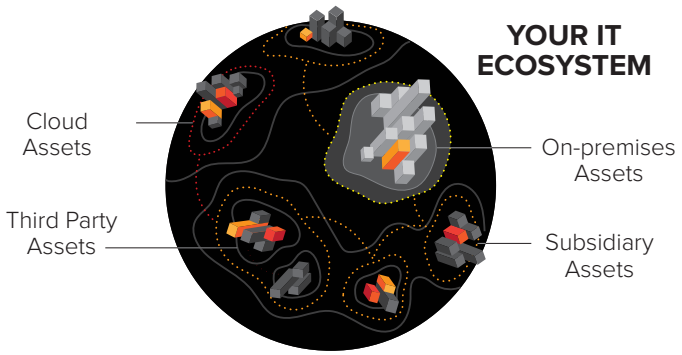

Figure 1. Your attack surface is the group of your *attacker-exposed assets*, known and unknown, wherever they are: in the cloud, in third-party environments, or in your subsidiaries.

[1] 2019 Verizon Data Breach Investigations Report, Figure 3

Most organizations have effective coverage against the second area with email security, endpoint security, and anti-phishing security and training solutions. But those same organizations — especially highly distributed organizations and those using cloud and as-a-service technologies — do not have full visibility to their attack surface and their attacker-exposed and soon-to-be-exploited assets. This paper focuses on the risk from your attack surface and how you can benefit from an assessment of your organization's security posture by viewing your attack surface from an attacker's point of view. .

Shadow risk, critical risk that is unseen or unmanaged by IT and security teams, is growing exponentially as applications, systems and infrastructure that used to sit within an organization's well-defined perimeter are now shifting — in part or entirely — to cloud and partner networks. The implications of this change are profound because every small misconfiguration in a cloud environment or a partner's network has the potential to open up access to your sensitive customer data, financial information and systems, application source code and intellectual property.

02 You Won't Find Shadow Risk Under a Streetlight

One approach popular among new CISOs assessing their organizations' security posture is to commission a penetration test. The challenge with penetration tests is that they are limited in:

- Coverage, providing visibility into a fraction of the entire attack surface
- Frequency, lasting just a few days or weeks and representing a point-in-time view
- Relevance, lacking an understanding of the business relevance of discovered issues

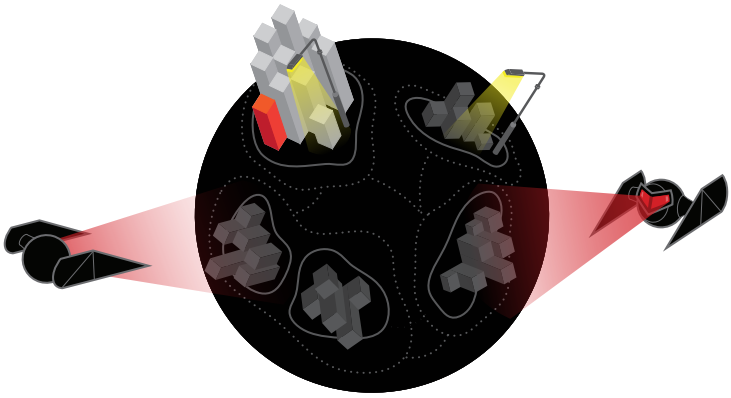

Figure 2. Attackers use advanced reconnaissance techniques that see more of your attack surface than the narrow view provided by legacy risk assessment solutions, depicted here as streetlights.

Likewise, vulnerability scanners are not designed to give you a complete picture and cannot help you identify unknown risks. They only know about the assets they are configured to scan, such as particular IP ranges or assets with agents.

> The way many organizations try to identify shadow risk is analogous to the well-known Streetlight Effect: looking in the dark for your lost keys under a streetlight, because that's where you can see best, even though you lost them elsewhere.

The first and foremost problem with these methods is that they ignore the way that attackers identify the blind spots in an organization's defenses and thus leave them exposed. They are also designed to be point-in-time, as opposed to continuous, and only do in-depth examination on a portion of the attack surface — a portion identified explicitly by an internal team member.

Using penetration testing and vulnerability scanners to map your attack surface is like looking under the streetlight for lost keys — it doesn't work well, it's just convenient.

03 **What's the Best Way to Take Stock Quickly?** The best and simplest approach for assessing the security posture of your new organization is to:

- Discover assets the way an attacker would
- Determine the business relevance of those assets
- Identify and prioritize attack vectors associated with the assets

And it's important to keep doing this assessment. Security isn't static. You should validate your security posture continuously as part of your new security program.

04 **CyCognito Platform Delivers Immediate and Ongoing Value** The CyCognito approach gives you immediate visibility to the breadth of your attack surface and the effectiveness of your security controls, without requiring any deployment or configuration.

The fully automated SaaS platform identifies:

- the entire attack surface, including assets that are managed outside the organization, to help you bring your shadow risk to light,
- the business relevance of those assets,
- and, ultimately, the most dangerous risks to your business, so you can remediate them first.

And unlike the legacy tools that give you a narrow and expensive point-in-time view that must be repeated periodically to be up-to-date, the CyCognito platform helps you validate your security posture automatically and autonomously on a continuous basis. The investment you make to get a picture of the security posture you inherited as a new CISO will continue to add benefit to your ever-changing organization and IT infrastructure as you build your security program.

Learn More

As a new CISO, you want to make sure that you are using the best tools that the industry has to offer in the most effective ways possible. Don't let the unknowns in your attack surface trip you up. Contact CyCognito to obtain your exclusive, and complimentary, attack surface map, to help you build a critical foundation for your security program.

CYCOGNITO
420 Florence Street
Palo Alto, CA 94301
cycognito.com

CyCognito is solving one of the most fundamental business problems in cybersecurity: the need to understand how attackers view your organization, where they are most likely to break in, and how you can eliminate that risk.