CYCOGNITO

SOLUTION BRIEF

BEST PRACTICES FOR MONITORING SUBSIDIARY RISK

Introduction

A key challenge for holding companies, multinational corporations and other conglomerates is monitoring the IT security risk of their subsidiaries. Subsidiary IT environments contain assets and networks that you don't manage but they can nevertheless put your organization at risk. In fact, unknown and unmanaged attacker-exposed assets in subsidiary environments can easily be the source of your organization's most critical cybersecurity risk. So, even if you lack chain-of-command authority over subsidiary IT, you still must ensure that your entire IT ecosystem is following security best practices in order to protect your organization's data, business, brand and reputation.

And of course the challenges of monitoring and eliminating risks in your subsidiary environments increases with the number of subsidiaries you have. Many global companies have hundreds or even thousands of subsidiaries under their corporate umbrellas.

Whether your organization has one or 1,000 subsidiaries, as a security executive, you should ensure that your team is adopting a process that addresses key questions in these areas:

Assessing Subsidiary Risks

How do we evaluate the scope of our risk from subsidiaries?

How do we identify the subsidiary assets and issues that the subsidiary teams may not even know about?

Measuring Their Security Posture

How do we prioritize subsidiary risks?

How do we measure their security status in alignment with our risk appetite?

Eliminating Critical Risks

How do we help our subsidiary teams understand where they should focus first?

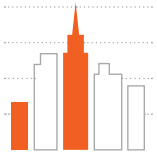
How can we provide guidance on the steps they should take to eliminate risks?

Monitoring Continuously

How do we continuously monitor our IT risks in existing or newly-added subsidiaries?

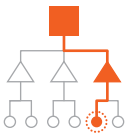
We recommend the following as best practices for monitoring and managing subsidiary risk:

Expose Subsidiary Risk



Measure Subsidiary Risk to Benchmark and Track Improvements

Help Subsidiaries Eliminate Their Critical Risks



Continuously Monitor Your Subsidiary Risk

01 Expose Subsidiary Risk

Every organization is subject to significant risk from unknown and unmanaged assets; our data shows that a full 25 to 75 percent of assets are unknown to organizations. This hidden risk is also known as shadow risk. Subsidiary environments are a significant source of shadow risk.

As a parent organization, you must ensure that your attack surface visibility fully embraces your subsidiary environments, even if they are not managed by the parent company's security and IT teams. And not only is it important to identify subsidiary assets, it's vital to understand how important each asset is to your business and to potential attackers to help you prioritize your response.

02 Measure Subsidiary Risk to Benchmark and Track Improvements

Building upon a strong foundation of discovering the attack surface of your subsidiaries and understanding the importance of each exposed asset, the next step is to objectively measure the security posture of each subsidiary. A baseline security score for each subsidiary, well-supported by details about how and why the score was assigned, provides you with objective content to use when you establish your top-level security program goals and approach each of the subsidiary teams who manage assets that are at risk.

03 Help Subsidiaries Eliminate Their Critical Risks

Unlike a third-party relationship, where you can walk away if a low security score is reported, your organization has a strong stake in making sure that your subsidiaries are quickly and efficiently resolving their security issues. Therefore, you need a method for:

Prioritizing the subsidiary risks that are identified: Security teams at subsidiaries simply don't have the time to wade through a lengthy, unprioritized list of vulnerabilities that is not paired with knowledge of the criticality of the asset or its desirability to attackers.

Detailing and communicating the remediation steps needed to address each issue: Increase efficiency by providing your subsidiary teams with actionable guidance about where and how each issue should be addressed.

Benchmarking and tracking subsidiary progress over time: Create an efficient process for tracking and reporting subsidiaries' security status.

04 Continuously Monitor Your Subsidiary Risk

Finally, you need a process for monitoring the always-changing security posture of each existing subsidiary, as well as any newly acquired ones. You want to be able to monitor continuously, detecting new assets, misconfigurations or exposures that may occur.

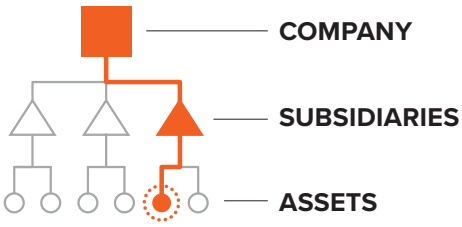


Figure 1. Risks in subsidiary IT environments create risk for the parent environment.

In addition to identifying new issues, your process should help you validate which of the risks that you flagged for remediation have been resolved. A solution with automation and scalability makes it efficient for you to monitor your subsidiaries, even if you have a thousand.

How CyCognito Helps You Assess and Eliminate Your Subsidiary Risk

The CyCognito platform is an automated, continuous, SaaS product that helps you assess, measure, remediate and monitor your attacker-exposed subsidiary environments efficiently and effectively. It:

- Discovers your subsidiaries automatically, needing only your parent company name to get started.
- Identifies subsidiaries' full attack surfaces, uncovering assets they didn't know existed, and providing the business context of each asset to prioritize risks.
- Objectively measures the risk of each subsidiary, as well as the risk of each asset in its environment.
- Provides detailed, actionable remediation guidance for each issue.
- Continuously monitors subsidiaries with an automated, scalable platform that needs no deployment or configuration.

Making sure that your subsidiaries don't increase your organization's IT risk is a critical task. Learn more about managing subsidiary risk effectively and efficiently at *cycognito.com*.

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.