Balbix®

NEW CISO ESSENTIALS™ SERIES

4 FACTORS to focus on in the FIRST 4 MONTHS

Modern enterprise CISOs are expected to “do it all” and as a new CISO, you’re going to want to hit the ground running as you are piecing together the foundational elements of your organization’s cybersecurity program.

The precedent you set and first impressions you make will determine how quickly you are accepted as a leader who can influence direction and deliver mission-critical outcomes.

It will also give you the headroom you need to settle into the “nuts and bolts” of your job (completing security posture assessments, getting to know key players, building political capital, nurturing relationships, and providing effective leadership).

Read on to see the 4 areas that should rise to the top of your list as you settle into your new job.

1 Get visibility into your security posture

A CISO's job is fraught with challenges which continue to increase as the enterprise grows in complexity. The enterprise attack surface is constantly expanding as organizations adopt digital transformation and cybersecurity has become a hyper-dimensional problem of extreme scale. The number and variety of vulnerabilities continues to explode. New and novel ways of compromising computer systems are discovered every day by security professionals as well as adversaries. Despite best efforts and robust technology investment, breaches are occurring with alarming frequency, oftentimes resulting in significant damage.

So how do new CISOs wrap their arms around these cybersecurity challenges and emerge victorious over the adversaries? With thousands of assets in your enterprise and each susceptible to a myriad of different attack vectors, there are millions of ways by which your enterprise can be breached. Your defense against the adversary is your enterprise cybersecurity posture. Therefore, understanding and defining the full scope of your cybersecurity posture is essential to protecting your business against breaches.

Security posture visibility essentially means having a complete and accurate picture of your security posture. This includes discovering and inventorying all your assets, monitoring them continuously to get an accurate picture of your risk, and the ability to easily access this information in the form of prioritized, searchable insights and action items. Visibility needs to be comprehensive and continuous, extending to all types of assets and security issues across an increasingly complex landscape.

Know what you're defending

An effective security assessment starts with an accurate inventory. You need to understand the various devices, applications, and services used across the enterprise: Who is using them and how are they being used?

Go above and beyond unpatched software

Because attackers use multiple attack vectors to compromise an enterprise, your cybersecurity assessment must cover all security issues, not just unpatched software.

Prioritize risks

Not everything in your network is equally important. Do not ignore or simplify the role of asset criticality in cybersecurity visibility, and make sure risks map to your business.

Establish a cybersecurity program framework

Security teams are pulled in many directions — vulnerability management, prioritization, incidence response, deployment and tuning of security tools, application security, dashboarding and reporting, to name just a few. In your first few months as CISO, you will need to establish a cybersecurity program framework and communicate that across the enterprise.

- **How will cybersecurity be managed?**
- **How will you know that you're working on the right projects?**
- **What are the most vulnerable areas of your attack surface?**
- **Can you quantify the progress you're making?**
- **Who are the key players and what are their responsibilities?**
- **What tools are in place and what more are needed?**

This is where you lay out your vision for keeping the enterprise safe. What are your goals and key cybersecurity strategies, and how do all of the moving parts fit together? What governance will be in place to keep everything and everyone on course (funding, corporate leadership, people, skillsets, integration, alignment)? And are your cybersecurity tools up to the task?

3 Communication with the Board of Directors

Your board members' view of cybersecurity is quite different from how security and IT team members think. Board members are primarily concerned with cybersecurity as a set of risk items, each with a certain likelihood of happening with some business impact. Your board also expects you to have a well thought out execution plan to transform your organization's cybersecurity posture to the recommended risk level.

- **You need to up level the conversation from cybersecurity to cyber-risk but stay tied to actual on-network cybersecurity posture.**
- **You must identify key areas of the business at risk from cyber-attacks, and help your colleagues understand how your cybersecurity program is aligned to this risk.**
- **At the board-level it is all about benchmarks, so you must have a sound mechanism to compare your cybersecurity posture and breach risk against similar organizations. Your board will look to you to recommend the appropriate level of residual cyber-risk your organization should aim for.**
- **You must have internal benchmarking data in your back pocket– what is working well, and what is not. And which groups have good cybersecurity posture vs ones that don't.**

Build relationships across stakeholders

Building relationships with lines of business and key stakeholders is an important success factor when you start any high-level job and it's particularly true for CISOs. Aside from your relationships with fellow executives and the organization's functional leaders, you will need to quickly connect with lines of business and key stakeholders such as Legal, HR, and others.

And you will need to get all risk owners to help with the cybersecurity mission. Whatever your organizational landscape, finding allies and teaming up with key players will be critical as you empower and leverage your co-workers to put their muscle behind managing cyber-risk across the organization.

How to empower all employees to manage cyber-risk better

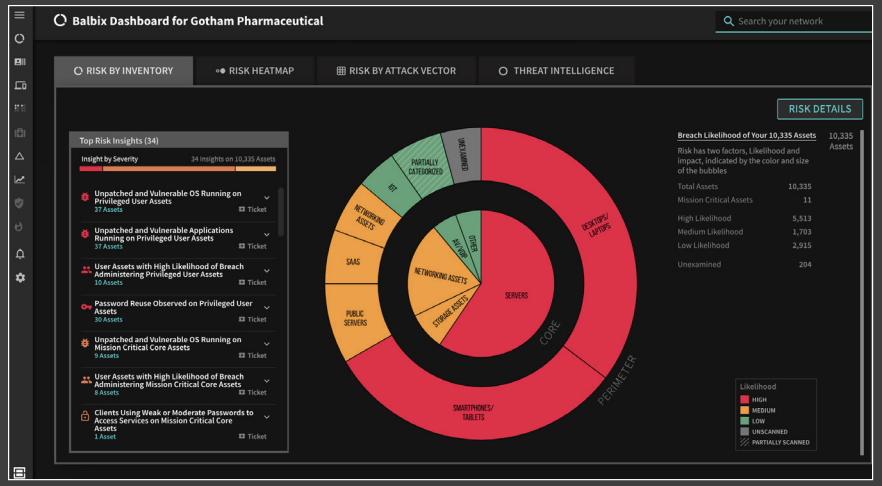
Individual risk owners are the first line of defense in any cybersecurity program. Being closest to the situation (and if provided with the right context and goals), they can be very effective in remediating risk. Here are some actions you can take:

- **Identify risk owners**
- **Communicate using automated notifications and digests**
- **Assign tasks with context, including options for mitigating risk**
- **Use points and incentives to gamify risk reduction and employ leaderboards**
- **Use tools that offer Integrations to ticketing and orchestration**

Towards a secure and cyber-resilient enterprise

New CISOs are “at the right place and the right time” to make a bottom-line difference for their organizations. They can drive the overall risk management strategy. They can provide the leadership needed to prioritize and manage cybersecurity risks. They can empower players across the enterprise to assume shared ownership of the cybersecurity mission. And they can put all of the pieces together to ensure a secure and cyber-resilient path going forward. It’s a difficult job, but one well worth the time and effort.

Balbix discovers and analyzes the enterprise attack surface to provide a 100x more accurate view of breach



Track your assets in real time through automatic discovery and continuous updates.

Automatically discover, analyze, and categorize all devices, apps, and services including managed and unmanaged, infrastructure, on-premises and cloud, fixed and mobile, IoT, ICS, etc.

Get answers to questions about your inventory, security posture, or breach risk using Google-like natural language search.

Customize your inventory and risk model based on your specific business needs to stay tightly aligned with the business.

Balbix®