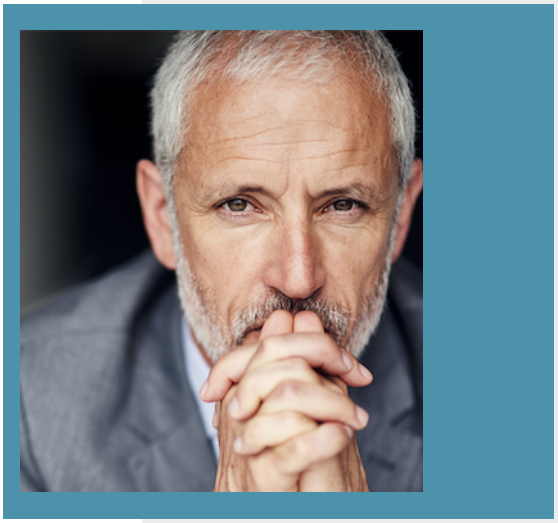
Balbix®

New CISO Essentials™ Series

TAKING STOCK OF THE ENTERPRISE SECURITY POSTURE TO HIT THE GROUND RUNNING

Introduction



The chief information security officer (CISO) is the executive responsible for steering an organization’s course through challenging and sometimes treacherous information, cyber, and data security landscapes.

This is easily said … but not so easily done. As cybersecurity attacks become ever more prevalent and continue to increase in sophistication, the U.S. and European Union are putting stronger privacy laws and security regulations in place. With successful breaches bringing increasingly serious consequences, today’s CISO is being asked “to keep the enterprise safe,” assuming a senior leadership role that is truly vital to the organization’s well-being.

No longer just compliance monitors and enforcers, CISOs need to be fully embedded within the business, highly knowledgeable about today’s shifting cybersecurity landscape, able to manage information risks strategically, and capable of creating a culture of shared ownership and accountability that drives cyber-resilience and best practices across the enterprise.

A Day in the Life

With such an ambitious charter, the CISO needs to wear many hats and be capable of juggling a number of balls at the same time. These include:

- Discovering, analyzing, and mitigating incoming threats
- Keeping abreast of emerging cyber-risks and regulatory requirements
- Ensuring that only authorized users have access to restricted assets
- Making sure IT and network infrastructure is as robust and agile as possible
- Overseeing investigations and forensics when things go wrong
- Building critical relationships within and outside the business
- Effectively communicating up and down the organization
- Providing strong leadership for all things cybersecurity

Positioning for success

The new CISO needs to bring to the job a blend of technical knowledge, business acumen, IT expertise, and cybersecurity skills in equal measure. CISOs also need to be comfortable in a leadership role that often goes head-to-head with other leaders within the organization, including C-Suite peers and the board.

Additionally, CISOs need the ability to understand the cyber-threat landscape for their industry along with related laws and regulations. They need to know how to leverage that knowledge as they identify risks and develop action plans to protect the business. They need to be great communicators. And equally important, CISOs need an appropriate position within the organization, one that supports their initiatives and allows them to deliver on their mandate.

Adding new moves to the old playbook

As a new CISO, early performance will be critical to success in your new role. In the first few months, you'll be assessed by colleagues and staff, judged as to your effectiveness, and tested as you present to your C-Suite peers.

The precedent you set and first impressions you make will dictate how your organization perceives you, and this will determine how quickly you will be accepted as the captain of your enterprise's "security ship.

What are your organization's top 2-3 security-related issues? These are top-of-mind from the CEO on down and delivering quick wins will establish your initial credibility. It will also give you the headroom you need to settle into the "nuts and bolts" of your job (getting to know key players, holding meetings, building political capital, nurturing relationships, and providing effective leadership that starts to make a difference right out of the gate).

In your first few months, focus on:

- Introducing yourself to the organization
- Establishing your credibility
- Building the right team
- Influencing and leading in a way that creates organizational cooperation and alignment
- Building momentum with early results

5

Crucial Steps

Here are 5 steps that will help you assume your new CISO leadership role with confidence as you start to build cyber-resilience within your organization:

1

Conduct a cybersecurity posture assessment

As a new CISO, one of the first tasks you'll want to tackle is an "as-is analysis." This will be the foundation on which you build your security program and strategy. You will also need to identify the risks your organization faces and its current cybersecurity posture. What's working and what's not? Who's on the team? Where do you begin? What budgets and metrics are in place? What are your organization's critical assets? And what is the best way to protect them?

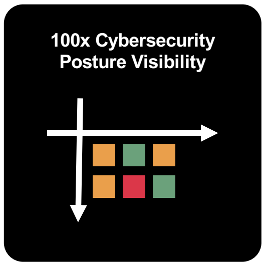
Gain real-time visibility into your attack surface and breach risk: Because the enterprise network is only as secure as its weakest link, your cybersecurity visibility must extend to all types of assets and all sorts of security issues.

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 they are 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.

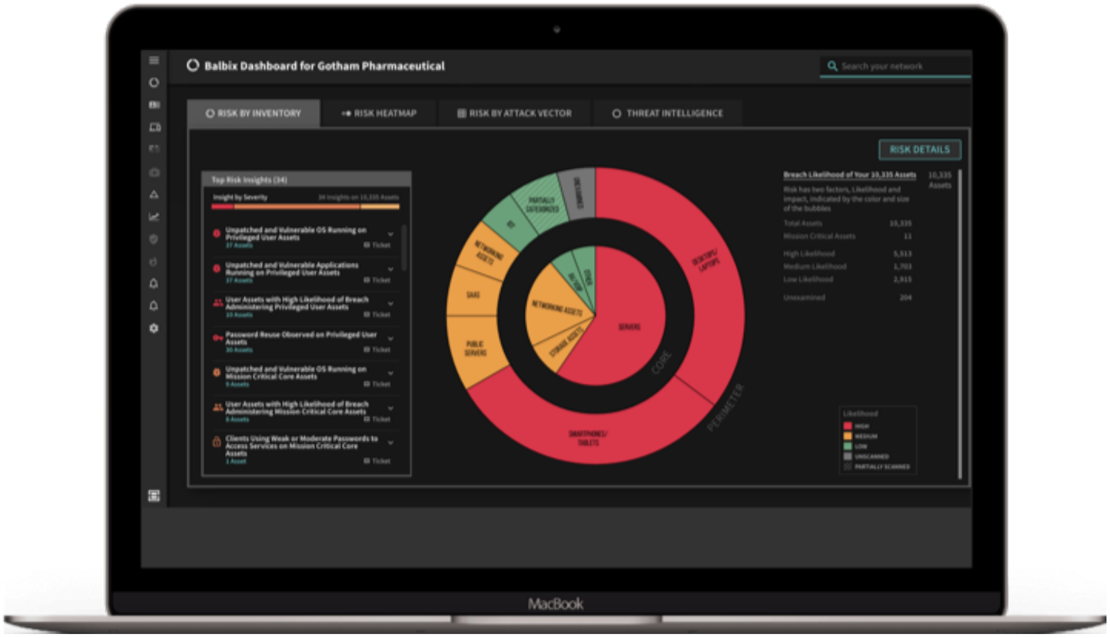
Learn more about visibility and prioritization


100x Cybersecurity Posture Visibility

Automatic Asset Inventory

Visibility and Security of IoTs, OT and Cloud Assets

Risk-Based Vulnerability Management



Balbix Dashboard for Gotham Pharmaceutical

Search your network

RISK BY INVENTORY | RISK HEATMAP | RISK BY ATTACK VECTOR | THREAT INTELLIGENCE

Top Risk Insights (34)

Insight by Severity — 34 Insights on 10,335 Assets

- Unpatched and Vulnerable OS Running on Privileged User Assets — 37 Assets — Ticket
- Unpatched and Vulnerable Applications Running on Privileged User Assets — 37 Assets — Ticket
- User Assets with High Likelihood of Breach Administering Privileged User Assets — 10 Assets — Ticket
- Password Reuse Observed on Privileged User Assets — 30 Assets — Ticket
- Unpatched and Vulnerable OS Running on Mission Critical Core Assets — 9 Assets — Ticket
- User Assets with High Likelihood of Breach Administering Mission Critical Core Assets — 8 Assets — Ticket
- Clients Using Weak or Moderate Passwords to Access Services on Mission Critical Core Assets — 1 Asset — Ticket

RISK DETAILS

Breach Likelihood of Your 10,335 Assets — 10,335 Assets

Risk has two factors, Likelihood and impact, indicated by the color and size of the bubbles

Total Assets	10,335
Mission Critical Assets	11
High Likelihood	5,513
Medium Likelihood	1,703
Low Likelihood	2,915
Unexamined	204

Automatic asset inventory

Traditional inventory method problems:

- They are labor-intensive, time-consuming, and hard to scale.
- Asset discovery is not real-time and continuous
- Enterprise security teams don't always control all assets, which makes gathering insights difficult.Typically only track managed assets, leaving assets like IoT and other non-traditional assets either undiscovered or partially tracked.
- Traditional inventory tracking tools miss the business context and business criticality of enterprise assets

The Balbix advantage:

- Track your assets in real time through automatic discovery and continuous updates.
- Balbix automatically discovers, analyzes, and categorizes all devices, apps, and services including managed and unmanaged, infrastructure, on-premises and cloud, fixed and mobile, IoT, ICS, etc.
- With Balbix, you can get answers to questions about your inventory, security posture, or breach risk using natural language search.
- The Balbix inventory and risk model can be customized based on your specific business needs and tightly aligned with your business.

2

Build key relationships

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

And you will need to get all risk owners in the organization to help with the cybersecurity mission.

Whatever your organizational landscape, finding allies and teaming up with key players will be a critical success factor as you empower and leverage your co-workers to take up the oars and put some muscle toward managing cyber-risk for the organization.

Learn more

Gamification of Cybersecurity Posture Transformation

3

Communicate your vision across the enterprise

Security teams are pulled in many directions–vulnerability management, incidence response, deployment and tuning of security tools, application security, dashboarding and reporting, to name just a few.

- Do you know if you are working on the right projects?
- Where are the riskiest areas of your attack surface?
- Can you quantify the progress you are making?

This is where you start to lay out your vision and a framework for keeping the enterprise safe. What are the goals 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)?

4

Assess team skills and identify gaps

CISOs rely are their technical teams to help navigate a safe passage as they fight the day-to-day cybersecurity battle. As a fresh set of eyes, the new CISO is in a position to spot development opportunities, skillset gaps, and perhaps better ways to organize for success.

Once your vision has been widely communicated, look for ways to bring performance to a whole new level.

5

Deliver key wins and spread the word

With a few early wins, you can set yourself up for longer term success. But these “wins” need to be selected carefully. Are they important to company leadership? Are these projects doable in your first six months? And will the impact of these wins be widely felt (e.g., by customers, by department heads, and/or up and down the organizational structure)?

The board member’s view of cybersecurity can be quite different from the security and IT team member’s view. Board members focus on higher level risks with significant business impacts, while front-line teams work the tactical issues.

- Board members and executives want to understand quantified breach risk.
- They want to know the level of acceptable risk that is appropriate for their organization.
- And they want to see a comparison with peer entities to grade performance and.

Balbix helps you quantify breach risk for top level execs and perform external benchmarking. You can also drill down from a business-level risk score into a risk heat map, which shows you the groups of assets that are driving the risk metric.

To help you develop a well thought out execution plan, Balbix prescribes prioritized actions that you can take to improve your network’s cyber-resilience and defense posture. Balbix also provides you with simulation tools that allow you to compare different fix plans.

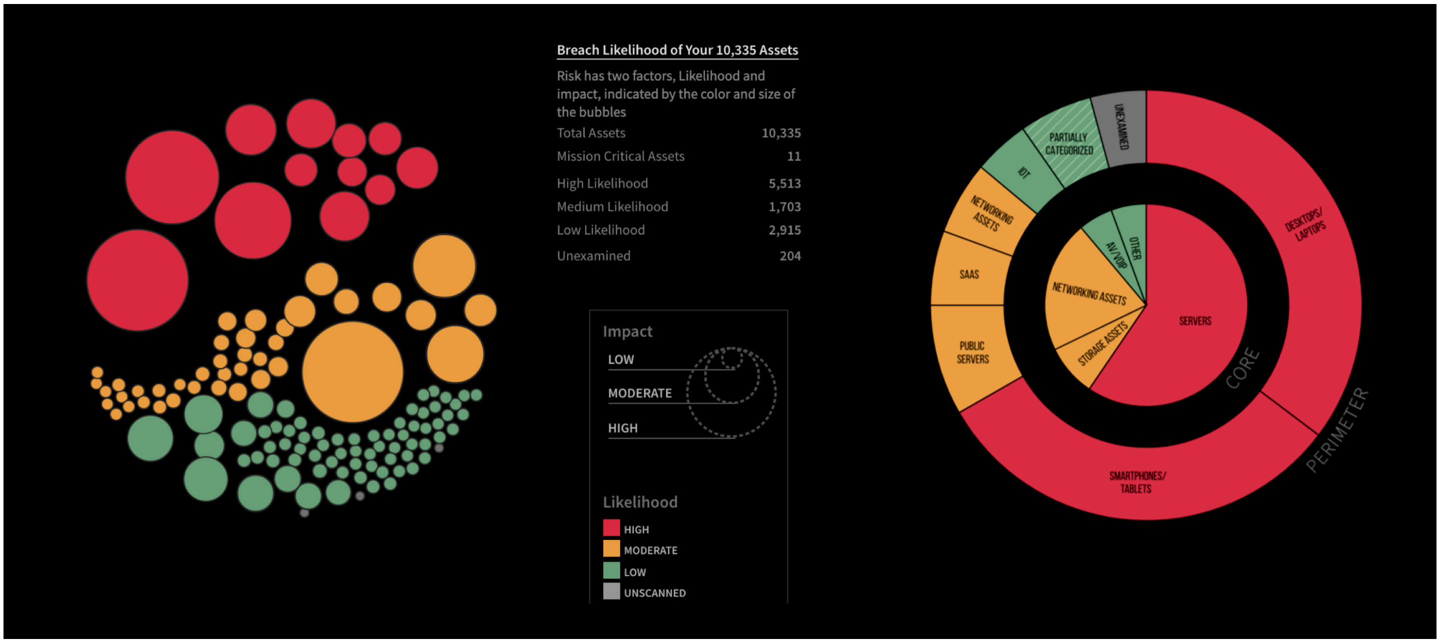
As an added bonus, Balbix allows you to generate board slides quite literally by hitting a button. The backup data is all there–you just click into a pie-chart to drill down and create your slide.

Learn more

Cyber-Risk Reporting for Board of Directors

Balbix BreachControl™

Balbix BreachControl platform uses specialized AI algorithms to discover and analyze the enterprise attack surface to give a 100x more accurate view of breach risk. Balbix enables a broad set of vulnerability and risk management use cases that help to transform your enterprise cybersecurity posture. The platform also provides a prioritized set of actions that you can take to transform your cybersecurity posture and reduce cyber-risk by 95% or more, while making your security team 10x more efficient.



Breach Likelihood of Your 10,335 Assets

Risk has two factors, Likelihood and impact, indicated by the color and size of the bubbles

Total Assets	10,335
Mission Critical Assets	11
High Likelihood	5,513
Medium Likelihood	1,703
Low Likelihood	2,915
Unexamined	204

AI-Powered Cybersecurity Posture Transformation

100x
more accurate
visibility
of breach risk

95%
or more
reduction
in breach risk

10x
improvement
in security
team efficiency

LEARN MORE

Hit the ground running

CISOs are expected to "do it all" when it comes to keeping their organizations safe. For a new CISO, it is possible to quickly understand the enterprise cybersecurity posture to hit the ground running as you embark on your new endeavor. Facing stiff privacy and regulatory requirements, increasingly sophisticated threats, an ever-changing IT landscape, and a heightened set of business risks, new CISOs need to do four high-level things really well:

- Elevate security to a board-level issue and keep it there
- Instill a culture of shared cyber-risk ownership across the organization
- Think strategically as they take needed tactical actions
- Partner with other key players to help navigate the choppy waters inevitably encountered on every cybersecurity journey

On a more tactical level, CISOs need to set their sights on:

- Achieving true visibility across the entire environment
- Hiring and retaining top talent
- Keeping cybersecurity priorities top-of-mind across the organization
- Maintaining a laser focus on security fundamentals
- Moving from a reactive to a proactive defense posture to keep the enterprise safe

Remember that your ultimate goal is to provide strong leadership as you step into "the CISO wheelhouse." These guidelines will help you navigate safe passage through both calm and threatening cybersecurity waters as you guide your organization toward a mature and resilient cybersecurity posture. For the new CISO, they should provide a set of best practices, let you know where to start, and give you a roadmap for ultimate success.

3031 Tisch Way, Ste 800
San Jose, CA 95128
866.936.3180
info@balbix.com
www.balbix.com