

CISO GUIDE

Where to Focus, When to Lead, and What to Follow

With cybersecurity increasingly becoming a board-level issue, there is immense focus on CISOs as they play a vital role in protecting the enterprise. It's a huge job and requires rare combination of skills and sensibilities. Whether leading or following, when it comes to security, CISOs are expected to "do it all." Read on to get some tips on where to focus, when to lead, and what to follow.



CISO RESPONSIBILITIES

Where to focus

1

Security architecture: Planning, buying, and rolling out security hardware and software, and making sure IT and network infrastructure is designed with best security practices in mind

2

Security posture visibility: Your visibility must extend to all types of assets and all sorts of security issues by continuously discovering your enterprise attack surface and understanding your defenses

3

Cyber-risk and cyber intelligence: Keeping abreast of developing security threats, and helping the board understand potential security problems that might arise from acquisitions or other big business moves

4

Security operations: Real-time analysis of immediate threats, and triage when something goes wrong and identity and access management which involves ensuring that only authorized people have access to restricted data and systems

CISO RESPONSIBILITIES

Where to focus

5

Program management: Keeping ahead of security needs by implementing programs or projects that mitigate risks — regular system patches, for instance

6

Data loss and fraud prevention: Making sure internal staff doesn't misuse or steal data

7

Investigations and forensics: Determining what went wrong in a breach, dealing with those responsible if they're internal, and planning to avoid repeats of the same crisis

8

Governance: Making sure all of the above initiatives run smoothly and get the funding they need — and that corporate leadership and the board of directors understands their importance¹

“

Boards are becoming increasingly interested in security and risk management; however, there's often a misalignment between what the board needs to know and what security and risk management leaders are able to convey.

”

- Rob McMillan, Gartner Research Director

By 2020, 100% of large enterprises will be asked to report to their board of directors² on cybersecurity risk at least once a year.

5 Security questions

Your board will inevitably ask these and you need to be prepared to answer

1

Are we 100% secure? Are you sure? Respond by reiterating that your team is identifying the highest-risk areas and allocating finite resources toward managing them based on business appetite³.

2

What happened at X company? How are we compared to others? Respond by discussing broader security responses such as identifying a similar weakness and how it's being addressed.

3

Do we know what our risks are? What keeps you up at night? Respond by explaining the business impact of risk management decisions and reassure the board that material risks are being adequately managed.

4

Are we appropriately allocating resources? Use a balanced scorecard approach in which the top layer expresses business aspirations and the performance of the organization against those aspirations.







5

How did this happen? What went wrong? Respond by acknowledging the incident, offer details on business impact, outline gaps and provide a mitigation plan.

When to lead

The CISO's critical balancing act








Like other executives in the company, CISOs need to know when to follow and when to lead. This is both a balancing act and a critical success factor as you juggle risks, trends, technologies, people, emerging threats, and the expectations of your board. Think of leading as it relates to all of your highest level responsibilities:

-  Defining the mission
-  Setting overall direction
-  Building a strong and diverse team and organization
-  Making the right strategic decisions
-  Networking with other security professionals
-  Reporting to, and in some cases sitting on, the board

What to follow

The CISO's critical balancing act

Think of following in areas such as:

-  Keeping abreast of current thinking and new technologies
-  Closely following and responding to the ever-changing security landscape
-  Putting together diverse multi-talented teams that can both follow and help lead the way
-  Speaking the board's language and communicating risk in board terms
-  Aligning to the board's high-level priorities
-  Investing in your people to influence direction, and deliver results
-  Tracking and adopting best practices

1. <https://www.csoonline.com/article/3332026/what-is-a-ciso-responsibilities-and-requirements-for-this-vital-leadership-role.html?nsdr=true>

2. <https://www.gartner.com/smarterwithgartner/5-security-questions-board-will-definitely-ask/>

3. <https://www.gartner.com/smarterwithgartner/the-15-minute-7-slide-security-presentation-for-your-board-of-directors/>

4

Actions for success

GAIN REAL TIME VISIBILITY

into your attack surface and breach risk and extend it to all types of assets and all sorts of security issues.

GET AN ACCURATE AND COMPREHENSIVE INVENTORY

of all devices, applications, and services used across the enterprise to know what you are defending.

GO ABOVE AND BEYOND

unpatched software because attackers use multiple attack vectors so cover other risk issues like password reuse, encryption issues, and misconfigurations etc.

GATHER ACTIONABLE INSIGHTS

by prioritizing vulnerabilities and ensuring that risks map to your business.

Click to learn more about visibility and prioritization



Balbix BreachControl™

The Balbix 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.

[LEARN MORE](#)

