10 rules for security leadership

Being a security leader is a serious role with high stakes.
Here are 10 rules you can follow to maximize your personal performance.

1 Understand what makes your organization tick

Take time to understand how your organization operates and generates revenue. What do your customers prioritize? What new product capabilities are coming? What's the company's future trajectory?

Knowing about both the business and tech will help you set relevant benchmarks and communicate in terms business leadership will support.

> *"Explain risks and their potential impacts — on reputation, revenue, and compliance — in framing and language that your board can understand. You know that every technical metric aligns with a business goal — make sure they know it, too."*
> — Cyber Defense Magazine

It's easier to set and communicate organizationally aligned goals when you...

2 Check your posture

Take inventory of your current security posture and environment so you can set priorities for meeting your benchmarks and goals. Be real with yourself and your team. What are your shortcomings? What are your blind spots? Do you have the data and platforms in place to make informed decisions and protect against a broad range of threats?

Attaining a firm grasp of where you are will help you identify where you need to prioritize your efforts, what partners you need to bring in, and what constitutes short- and long-term success.

When you know where you're headed, you can...

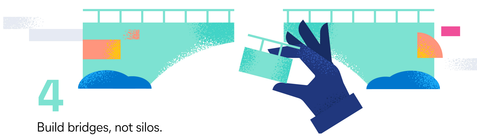
3 Embed security into the business function

Security can often be perceived as a hurdle for other departments looking to "move fast and break things." As CISO, you're all too familiar with the consequences of security not being an integral part of initial planning discussions.

Ease any potential friction by building a culture of "we" "yes, and..." within your own team, so that others seek to engage security early on. When you can show the business value of a secure product, it's much easier to define security's role and seamlessly integrate into your organization.

> *"... 69% of employees have bypassed their organization's cybersecurity guidance in the past 12 months... 74% of employees said they would be willing to bypass cybersecurity guidance if it helped them or their team achieve a business objective."*
> — Gartner

Your role is all about people, so ...



4 Build bridges, not silos.

Create relationships across your organization to build trust, know who you can turn to for support when needed, and communicate more effectively.

Cross-department connections make it easier for you to cultivate a culture of security and keep others engaged, so they'll identify potential risks earlier and proactively pull you in to address them.

> *"For the modern CISO, the key to successfully mitigating risk is to completely embed security throughout the enterprise. But before we can embed a security mindset in another business unit, we need to create connections, generate buy-in, and build trust with key stakeholders."*
> — Security Magazine

This will help ensure your organization can...

5 Remember the fundamentals

The biggest problems sometimes arise when we're so focused on advancement that we miss the basics. Don't neglect your existing systems for the new shiny tool.

Your organization's chain of security is only as strong as its weakest link, so security awareness among your organization's employees and contractors is essential. Make it fun and personal. You could even offer incentives for colleagues who report suspicious phishing attempts.

Other essential fundamentals include changing default configurations, removing unnecessary components, patching, and more. Your security approach should scale from common sense to complex.

The security landscape is changing fast, so...

6 Never stop learning

It's crucial to stay on top of current trends, vulnerabilities, threats, and advancements in cybercrime (like the use of generative AI). Invest some of your — and your InfoSec team's — time into industry research and ongoing education. Learn about the latest security tools and platforms and identify current best practices to stay ready for what's next.

> *"We have barely scratched the surface of AI's potential, positive and negative. CISOs not only have to contend with the technology's immediate impact, but they also must prepare for how it will shape their responsibilities in the future."*
> — Information Week

A good way to do this is to...

7 Get to know others facing the same challenges

No one CISO can do everything alone. Being a part of the larger security community offers opportunities to collaborate, get (and give) advice, and keep up with the latest security issues facing others in your position.

> *"Next-gen CISOs regularly participate in industry events and often share their experiences across social media as well as broadcast and print media, helping to further their reputation and influence."*
> — CSO Online

Tackling those issues is easier when you...

8 Stay nimble and anticipate change

The best-laid plans rarely go off without a hitch. Stay open to change so you can quickly adapt your strategies and priorities when needed.

Do you have contingency plans in place for common situations? Which of your processes are the least adjustable? Can you take steps to change them now so you're ready when you need to act fast? What parts of your infrastructure are keeping you from being as nimble as possible?

Practicing mock scenarios with your team can help strengthen incident response and expose any weaknesses in your process.

And remember, you work with capable people, so...

9 Stay out of the weeds and delegate

Knowing what's happening in your organization and staying on top of potential issues is essential, but trust your team members to do their job. And tap into your cross-department and partner relationships to help when needed.

Clearly establish roles and responsibilities upfront to ensure everyone understands what security-focused decisions they're empowered to make on their own. Then you can stay strategic and focused, knowing they'll pull you in at the right times.

> *"Modern development practices focus on smaller and smaller blocks of responsibility so no one person can have a complete handle on every aspect of an application."*
> — CSO Online

But keep tabs on any issues that arise. Especially when it comes to vendors...

10 Hold your vendors accountable for security

Third-party due diligence ultimately falls on you. Your vendor partners play a critical role in your organization's ability to keep your users safe and secure. Make sure they're delivering what you need by asking questions like:

- What security measures are currently in place?
- What is their approach if a security issue is identified in their product or service?
- Does the vendor have a business continuity plan?
- How soon will the vendor notify you in the event of a breach?