2022

The "Office of the CISO": A Framework for Chief Information Security Officers

Yael Nagler
YassPartners.com

Christophe Veltsos
Minnesota State University, Mankato, christophe.veltsos@mnsu.edu

The "Office of the CISO":

A Framework for Chief Information Security Officers

by

Yael Nagler
YassPartners.com

Chris Veltsos
MSU Mankato

The Office of the CISO framework outlines and integrates three key elements required to operate at an 'executive' level, in the context of the CISO role. Chief Information Security Officers (CISOs) are more impactful, and their programs are more effective, when they are delivering at a higher caliber of 'executive.'

Introduction: The CISO is Also an "Office"

As we enter 2022, cybersecurity continues to challenge corporations and their CISOs. The sophistication of cyberthreats coupled with an evolving digital landscape has resulted in increased complexity and expanded responsibilities for the CISO. Simply put, there is greater scrutiny[1], greater regulation[2], greater complexity[3], and greater scope[4] than ever before.

To respond to these changes, CISOs must organize their "Office of the CISO" to meet the expectations and deliver for their organizations. Whether the CISO has a staff of three or thirty and whether they are prepared or not, these elements are being increasingly expected of CISOs. You can think of it as, 'executiv-izing.'

[1] NATO Cooperative Cyber Defence Centre of Excellence https://ccdcoe.org/research/

[2] Quantum Computing and Cybersecurity by the Belfer Center at the Harvard Kennedy School https://www.belfercenter.org/publication/quantum-computing-and-cybersecurity

[3] Global Risks Reports from the World Economic Forum https://www.weforum.org/global-risks/reports

[4] Verizon Data Breach Investigations Reports https://www.verizon.com/business/resources/reports/dbir/

This article lays out a three-part framework for the Office of the CISO.

How Do You Know You Have an “Office of the CISO” Problem?

You may have an Office of the CISO problem if you’ve experienced any of these pain points:

- You have at least one difficult executive relationship. *Is it Engineering? Network Ops? Audit? Cloud Security? Legal? Other?*
- You were recently asked by Legal “what’s our risk?” and you aren’t sure that you nailed the response.
- You know you have to give an update to executives, but you aren’t sure what they want to hear about, what level to share information at, and how to best communicate what you have to say.
- You don’t know much about each of your board members. *Where have they worked in the past and what is their role on the board?*
- You’re unable to produce an ad-hoc update on a key security metric or alert in under 30 minutes.
- You know you need to buy some service, product, or insurance but you know there’s little chance that the powers that be will approve that expense.
- Your Sunday nights feel stressful, or is it Wednesday mornings?

The good news is that you aren’t alone in feeling these pain points. These are not your typical technology stack related issues… but they all have one thing in common: how you, as a CISO, operate your Office of the CISO, and thus how you structure your interactions with the rest of your organization’s leadership.

The 3 Pillars of the Office of the CISO

Whether it is a growing company or a global enterprise, the Office of the CISO exists. Below, we've organized the activities into 3 core functions. How you operationalize each activity should be tailored to your organization's needs.

1. Strategy, Governance & Oversight

The Office of the CISO is expected to be aware of and involved in:

- Company Policies & Regulatory Requirements → Aligning policies with the organization's practices and external expectations is rule #1 of the CISO. Pay attention to: information protection, computer usage, system access, and risk management.
- Enterprise Risk Management → The cybersecurity function should be actively supporting the company's risk treatment processes. Pay attention to: risk acceptances, risk exceptions, and risk and control action plans.
- Client RFP Response & Certifications → Scaling and responding to inquiries from external stakeholders such as clients or auditors makes security a better partner of the business. Consider increasing speed and consistency when responding to inquiries.
- Audits & Pen Tests → These are going to happen and should be invited. Actively engage with the assessor to explain, clarify, and validate findings, risks, and controls. These reviews provide objective visibility and shape the discussions around risk tolerance and investment. They should be carefully planned and executed.
- Departmental Budget & Security Strategic Plan → Being able to articulate a clear business case is the cost of entry to the executive level and demonstrates company alignment, which earns the CISO trust when discussing risk. Have a specific plan and a clear view of business (e.g. expenses and headcount), both those of the security function and that of the whole organization.

While these activities frequently challenge CISOs, they are components of every program. CISOs should walk into their office anticipating that they will have to address these elements and be prepared to quantify and measure the output of each.

Incidentally, doing these tasks well shows their peers that the CISO is a strategic business executive.

2. Talking & Partnering

CISOs should expect that they have a responsibility to lead the company's narrative around security and risk. Rather than grumbling about what has been said, CISOs should take ownership for framing the message and engage at key levels of the organization.

Specifically, the Office of the CISO prioritizes and influences the following:

- User Experience Changes → Changes that impact the end user need to be communicated for greatest impact. Consider not just the message but also the scheduling and sender to influence how the message will be received. *Sure, it's PR. PR that goes a long way to getting people on board.*
- Executive Escalation → Use the same rigor in escalating industry headlines and security successes as used to provide crisis notifications. Reliably providing timely updates simultaneously creates a common language and reassures executives that security "tells me when I need to know something."
- Board Reporting → The relationship with the board is a value-add for a CISO and should not be a chore. In preparing the materials and updates for the board, CISOs should consider how to best unlock the value of the Board's insight. Consider, structure, sequence, message, and desired outcome.
- Government Relations and External Policy → CISOs have a responsibility to be involved in and to track external trends, and to represent their company's interests. Whether it be law enforcement, ISACs, NIST, MITRE, think tanks or peer communities, following and participating (or not participating) is a decision the CISO is making and possibly, a statement about the company's security program.

Context setting is the foundation for strong communications. The CISO doesn't need to "own" every cybersecurity or cyber risk related communication, but they do have a responsibility to be actively involved in their messaging.

Investing in establishing relationships — during 'peace-time' — with stakeholders will make partnering easier during times of stress.

3. Operations

Maintaining security is also about robust operations. The office of the CISO integrates and threads the needle across relevant operations:

- Project Management → There are always projects. When it's not business as usual, it's a project. Having a consistent way of raising a project through to project close-out reduces friction and increases productivity. It's an activity that affects almost every part of the team in some way and benefits from clear processes and templates. Much as every organization is now a digital business, every project now has a cybersecurity angle.
- Recruiting, Onboarding & Promotion → This is not a joke. How we write job descriptions, onboard, career path, and manage performance should not be delegated entirely to each individual manager. It is the responsibility of the CISO to set the tone and energy of the team, no matter the size of the team. Practices should eventually be created for: interviewing, onboarding and training, team integration, promotion criteria, objective setting, talent reviews.
- Alert Tuning → Whether it's the SOC, NOC, Helpdesk, or Fusion center, alerts are being defined and monitored. Having a practice of reviewing and tuning keeps them fresh and meaningful. This is your opportunity to increase the signal to noise ratio.
- Crisis Preparedness & Testing → One thing is true, we don't know what we don't know. To continuously be prepared for a crisis, CISOs must challenge how their program reacts in simulation. Maturing preparedness requires testing more than the technology. We must challenge our teams to think beyond what has already occurred and challenge the status quo.

Operational complacency is a common and unseen risk. The best preventative control is to continuously tune alerts, and respond to requests and projects in a timely manner.

Conclusion

CISOs today are expected to anticipate, message, and respond to a wider range of topics in a shorter time frame with greater consequence. Developing an Office of the CISO mindset & practice enables the CISO to deliver with greater impact. How a CISO organizes and staffs — as well as prioritizes — their office of the CISO will vary.

To figure out where to start, CISOs should ask themselves:

1. Are we continuously tuning and ready to respond? Are we doing what we say we want to be doing if we're doing it well?
2. Is the story that I'm telling the right one for each audience that I'm speaking to?
3. How are we quantifying and communicating these things?
4. Do I feel confident that we are anticipating the right things?
5. Am I "executiv-izing" at the same level as the executive leadership?

Final word of encouragement: starting and improving is better than not starting. Whether you start with the easiest thing to improve or start with the thing that needs the most help, you have made a positive stride forward in elevating your Office of the CISO.