Rise of the Chief Intelligence Officer (CINO)

anomali.com/blog/rise-of-the-chief-intelligence-officer-cino

Anomali Sr. Director of Cyber Intelligence Strategy A.J. Nash recently penned a column for United States Cybersecurity Magazine about how changing security challenges call for new skillsets and leadership professionals, who can help to develop ad run new programs that keep pace with modern adversaries. In "Rise of the Chief Intelligence Officer (CINO)," A.J. makes a case for why this position is needed and what such a leader's skill set and experience should include. It is republished here in its entirety and with full permission.

In response to growing threats in cyberspace, private sector organizations began creating Intelligence programs nearly a decade ago, usually referred to as Cyber Threat Intelligence (CTI). In theory, the private sector was attempting to replicate what the government has successfully done for generations: gain informational advantage to prevent enemy victories and mitigate damage from enemy successes. While most large enterprises today have some sort of a CTI program, the majority are using the word "intelligence" without the tradecraft, standards, or processes to support the label. "Intelligence" in the private sector is still primarily tactical and technical cybersecurity led by people with backgrounds to match. Best practices for collection, production, and dissemination of intelligence are rarely known by those charged with the responsibilities of an intelligence organization. Moreover, only a handful of companies have integrated intelligence into enterprise-wide processes for optimization of outputs that meet documented organizational goals and objectives. Instead of being intelligence-driven security practices, much of the private sector remains underinvested and underprepared. Worse yet, most organizations with CTI programs, even effective ones, restrict their own ability to capitalize on the time and money invested in CTI because their vision for Intelligence is limited to the Security Operations Center (SOC).

The root cause for these challenges is a fundamental misunderstanding of intelligence, borne out of ignorance for the differences between Cybersecurity and Intelligence as independent career fields. Instead of being focused on Indicators Of Compromise (IOCs), signatures, and response actions, Intelligence should be a means of countering threats, cybersecurity or otherwise, and driving enterprise-wide improvements in risk reduction.

The answer to this challenge is to capitalize on the lessons learned by the U.S. Government (USG) regarding Intelligence. Just as there is a Director of National Intelligence (DNI) who reports directly to the President and leads the U.S. Intelligence Community "in intelligence integration, forging a community that delivers the most insightful intelligence possible,"[1] private sector enterprises each need a single Intelligence leader reporting directly to the CEO, President, or Board of Directors. Instead of the sole intelligence function of a company being a CTI team buried inside the SOC and focused on defensive cyber operations or the needs of the Chief Information Security Officer (CISO), establishment of the Chief Intelligence Officer (CINO) will enable companies to maximize the value of their investments, eliminate redundancies, and reduce risk.

In the 1980's, as C-suites expanded to include Chief Information Officers (CIO),and in the 2010's, to include Chief Security Officers (CSO) and Chief Human Resources Officers (CHRO), it is time to open a new seat at the table for the first Chief Intelligence Officer (CINO).

The Ideal CINO Candidate

When adding a chair in the boardroom, it is important to assess what unique value the new addition will bring to the Executive Staff (E-Staff). The skills and experiences needed for the newly minted CINO start with a deep knowledge of traditional intelligence standards and practices as well as impeccable integrity and judgement. This will be the senior expert on Intelligence and an influential voice informing the E-Staff and the Board; sometimes influencing trajectory-changing corporate decisions. Beyond that, a successful CINO will need a strong understanding of cybersecurity standards and practices, as well as familiarity with physical security concepts, a background in risk assessment and reduction, a mindset for business priorities, a process-driven approach, emotional intelligence to build relationships across business lines and partnerships, and a strategic outlook.

While locating someone with all (or even most) of those skills will not be easy, the impact of the role warrants finding or growing someone capable of demonstrating all these characteristics. The most qualified candidates will be Intelligence leaders in the private sector who transitioned from the government, as they will have Intelligence tradecraft expertise and understand what drives private enterprise.

Relationship Between the CINO and Executive Counterparts

A typical E-Staff consists of (see Figure 1) the Chief Executive Officer (CEO), Chief Financial Officer (CFO) Chief Operations Officer (COO), Chief Information Officer (CIO), Chief Customer Officer (CCO), Chief Marketing Officer (CMO), Chief Product Officer (CPO), Chief Human Resources Officer (CHRO), and Chief Security Officer (CSO). Subordinate to the CSO is usually the Chief Information Security Officer (CISO), although that role is sometimes merged with either the CSO or CIO roles.

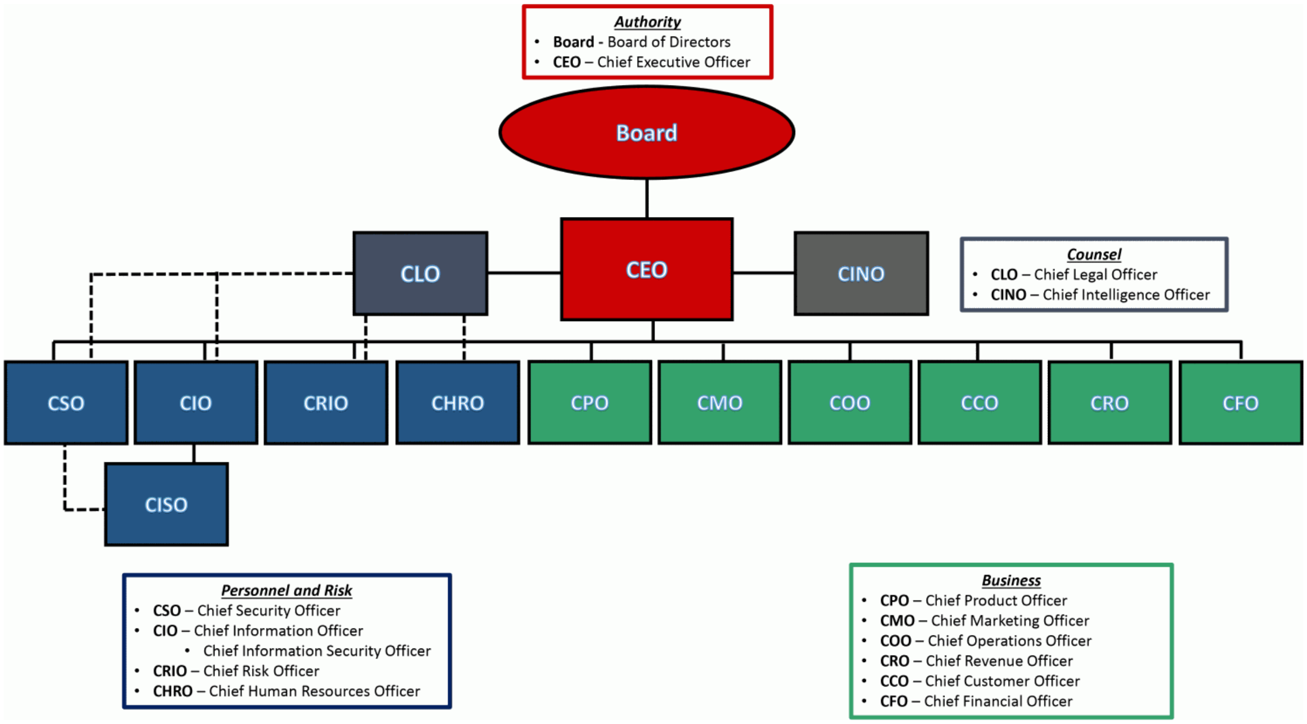
Authority
Board - Board of Directors
CEO – Chief Executive Officer
Board
CLO
CEO
CINO
Counsel
CLO – Chief Legal Officer
CINO – Chief Intelligence Officer
CSO
CIO
CRIO
CHRO
CPO
CMO
COO
CCO
CRO
CFO
CISO
Personnel and Risk
CSO – Chief Security Officer
CIO – Chief Information Officer
Chief Information Security Officer
CRIO – Chief Risk Officer
CHRO – Chief Human Resources Officer
Business
CPO – Chief Product Officer
CMO – Chief Marketing Officer
COO – Chief Operations Officer
CRO – Chief Revenue Officer
CCO – Chief Customer Officer
CFO – Chief Financial Officer

Figure 1: Relationship between the CINO & Executive Counterparts

The CINO, like the rest of the E-Staff, will be equal to all except the CEO to whom all others report. If the CISO is subordinate to a CSO or CIO, it is the CSO or CIO who is the CINO's peer; not the CISO. It is important to note that, as Intelligence is a service and not a product, the CINO will view their peers as customers; therefore, will only take direction from the CEO. Other roles that may or may not exist include Chief Customer Officer (CCO), Chief Risk Officer (CRIO), and Chief Legal Officer (CLO) for those with inside counsel."

Role and Responsibilities of the CINO

Serving as the authority on Intelligence, the CINO will have five main responsibilities to the enterprise. They are as follows:

- **Establishment, Enforcement, and Socialization of Intelligence Standards and Tradecraft:** The CINO will be responsible for establishing and enforcing analytic standards and tradecraft based on established best practices. These will include adopting Intelligence Community Directives (ICDs) 203,[2] 206,[3] and 208,[4] structured analytic techniques,[5] the Traffic Light Protocol,[6] and the use of frameworks such as MITRE ATT&CK,[7] Cyber Kill Chain,[8] The Diamond Model of Intrusion Analysis,[9] National Institute of Standards and Technology (NIST) Cybersecurity Framework,[10] and Factor Analysis of Information Risk (FAIR).[11] Furthermore, as Intelligence is only effective if the receiving parties understand the messages delivered from the Intelligence team, the CINO will be responsible for training on the language of intelligence, including confidence language, caveats, and source validation.
- **Creation and Maintenance of Intelligence Requirements:** The CINO will be responsible for research and analysis of existing operations, processes, goals, objectives, systems, and personnel for the purpose of authoring, validating, and maintaining Enterprise Intelligence Requirements (EIR) that reflect the strategic needs of the business. Furthermore, the CINO will develop and maintain Subordinate Intelligence Requirements (SIR) for individual entities across the enterprise. Finally, the CINO must map all SIRs to established EIRs to eliminate the tendency to expend energy on wasteful efforts against interesting but valueless intelligence projects (known as “shiny objects”).

- **Delivery of a Unified Intelligence Picture:** The CINO will be responsible for the entire Intelligence Cycle, (Figure 2) with the output being the delivery of Intelligence that creates informational advantages, drives proactive organizational changes, and reduces risk across physical security (including facilities, personnel, and executive protection), cybersecurity (offensive and defensive), insider threat, Governance, Risk and Compliance (GRC), Mergers and Acquisitions (M&A),brand protection, and crisis communications. Beyond delivering intelligence to each of these customer organizations, the CINO will be in the unique position to synthesize intelligence responding to EIRs and SIRs. What's more, the CINO will be making connections that today's enterprises are unable to see due to duplication of efforts, stove piping, parochialism, political rivalries, and individuals who prioritize personal career objectives over the needs of the enterprise.

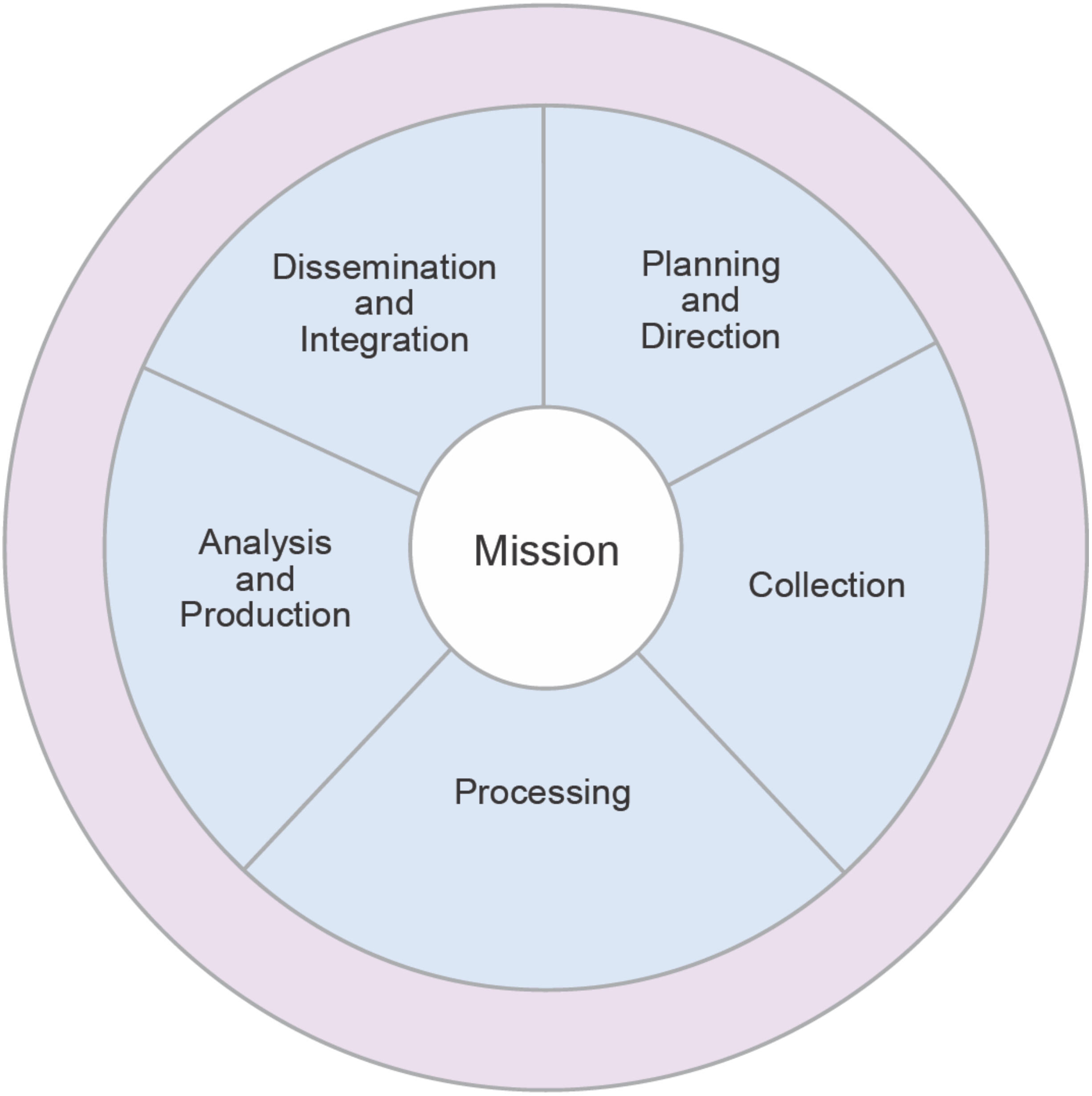

Figure 2: Intelligence Process

- **Proactive Intelligence:** The CINO will be responsible for delivering assessments and estimates regarding threats and risks, including probabilities and recommended courses of action for proactive or reactive responses, to executive leaders and peers. This intelligence can include both actionable intelligence (meant to inform or drive immediate or near-term decisions) and informational intelligence (meant to educate on patterns, trends, or understanding needed to grow an overall body of knowledge that can serve as the foundation for later actionable intelligence production).
- **Response Intelligence:** The CINO will be responsible for supporting ad-hoc operations within any supported function, to include, but not limited to, physical or cybersecurity incident response, and insider threat investigation. The intelligence produced in response to these security operations should seek to improve understanding of the threats, risks, and recommended courses of action for minimizing loss and protecting business interests.

Benefits of a Top-Down Approach to Intelligence

Elevating Intelligence and establishing an independent CINO who will report directly to the CEO will yield some clear benefits over today’s more common model of CTI buried inside a SOC. First, Intelligence will no longer be disproportionately influenced by the needs of one organization at the expense of other organizations. Serving under the CEO will empower the CINO to objectively assess EIRs and SIRs; therefore, recommending prioritization based on the strategic vision of the CEO without subordinate organizations or leaders forcing Intelligence to prioritize their needs over all others. This ensures that an enterprise will capitalize on the significant investment in talent, access, and technologies needed to create an effective Intelligence program. Second, with Intelligence elevated and unified, the CINO will be able to reduce redundancies in expenditures and effort that often plague large enterprises today. For instance, many enterprises currently have multiple teams paying for the same or similar intelligence from vendors. This is often caused by one of the following factors:

- Inefficient or bypassed procurement processes
- Ignorance among teams of the roles and responsibilities of their counterparts
- Managers prioritizing personal objectives over the needs of the enterprise

Third, with Intelligence unified under the CINO, the enterprise will benefit from having a single authoritative source. In time-critical situations, including security, cybersecurity, and business crises, competing opinions of varying validity based on inconsistent information and judgement criteria lead to poorly informed decisions that can be catastrophic. The CINO will act as a unifying agent across all available sources, serving as trusted and reliable counsel to the CEO and E-Staff at the most critical times.

Visualizing the Future of Intelligence in Private Industry

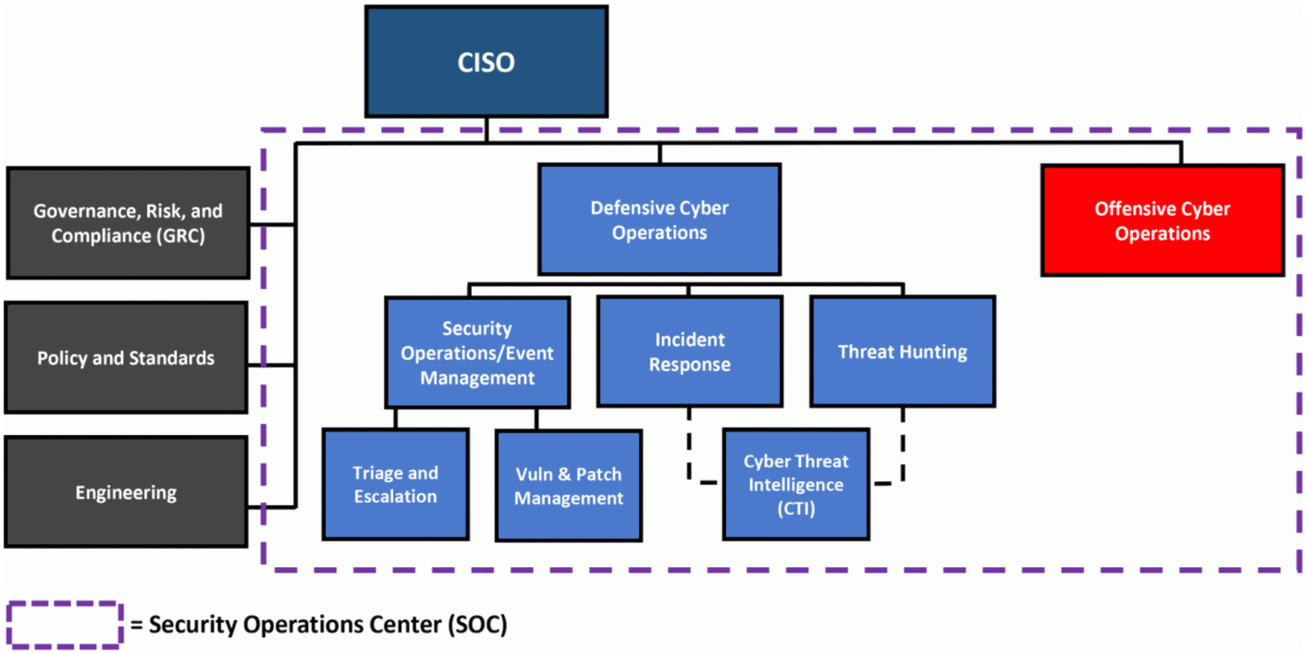
CISO
Governance, Risk, and Compliance (GRC)
Policy and Standards
Engineering
Defensive Cyber Operations
Offensive Cyber Operations
Security Operations/Event Management
Incident Response
Threat Hunting
Triage and Escalation
Vuln & Patch Management
Cyber Threat Intelligence (CTI)
= Security Operations Center (SOC)

Figure 3

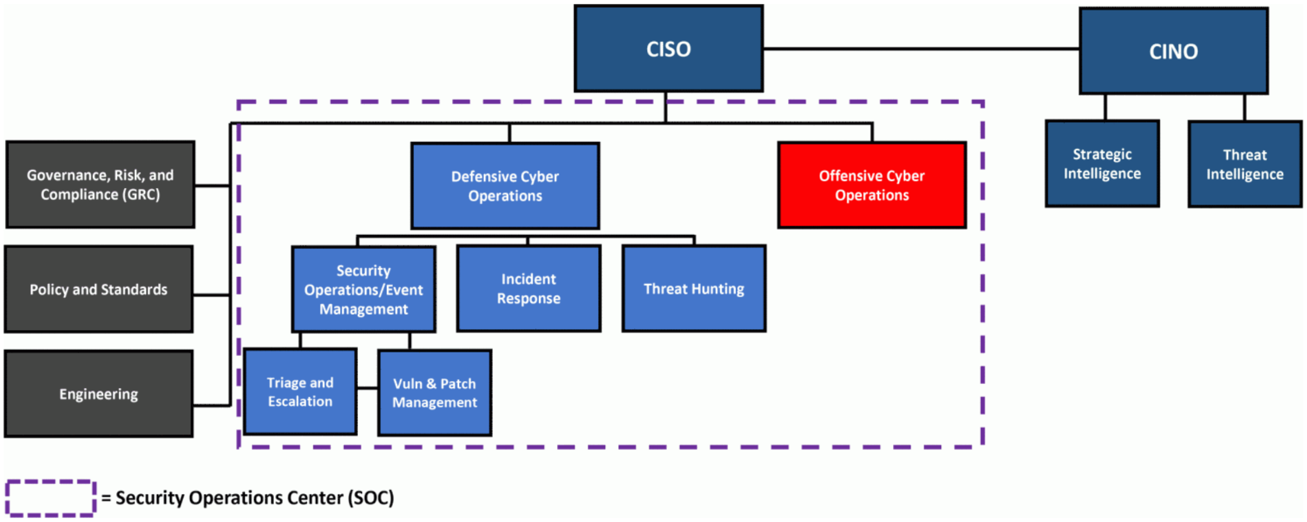
CISO
CINO
Governance, Risk, and Compliance (GRC)
Policy and Standards
Engineering
Defensive Cyber Operations
Offensive Cyber Operations
Security Operations/Event Management
Incident Response
Threat Hunting
Triage and Escalation
Vuln & Patch Management
Strategic Intelligence
Threat Intelligence
= Security Operations Center (SOC)

Figure 4

Having established the role, responsibilities, and benefits of expanding the E-Staff to include the CINO, the remaining question is who will report to the CINO and how that will change existing organizations. This is likely the easiest adjustment to make, as most organizations are mature enough to move to the CINO concept, and already have established effective CTI programs. Transitioning from CTI within a SOC to Intelligence under a CINO is just a matter of elevating the current team and expanding their mandate to match the program described previously. Figure 3 and 4 (see above) offers a visualization of these current and future states of Intelligence.

References

[1] https://www.dni.gov/index.php/who-we-are/mission-vision

[2] https://fas.org/irp/dni/icd/icd-203.pdf

[3] https://fas.org/irp/dni/icd/icd-206.pdf

[4] https://fas.org/irp/dni/icd/icd-208.pdf

[5] https://www.cia.gov/static/955180a45afe3f5013772c313b16face/Tradecraft-Primer-apr09.pdf

[6] https://www.first.org/tlp/

[7] https://attack.mitre.org/

[8] https://www.lockheedmartin.com/enus/capabilities/cyber/cyber-kill-chain.html

[9] https://www.activeresponse.org/wpcontent/uploads/2013/07/diamond.pdf

[10] https://www.nist.gov/cyberframework

[11] https://www.fairinstitute.org/fair-risk-management

Topics: