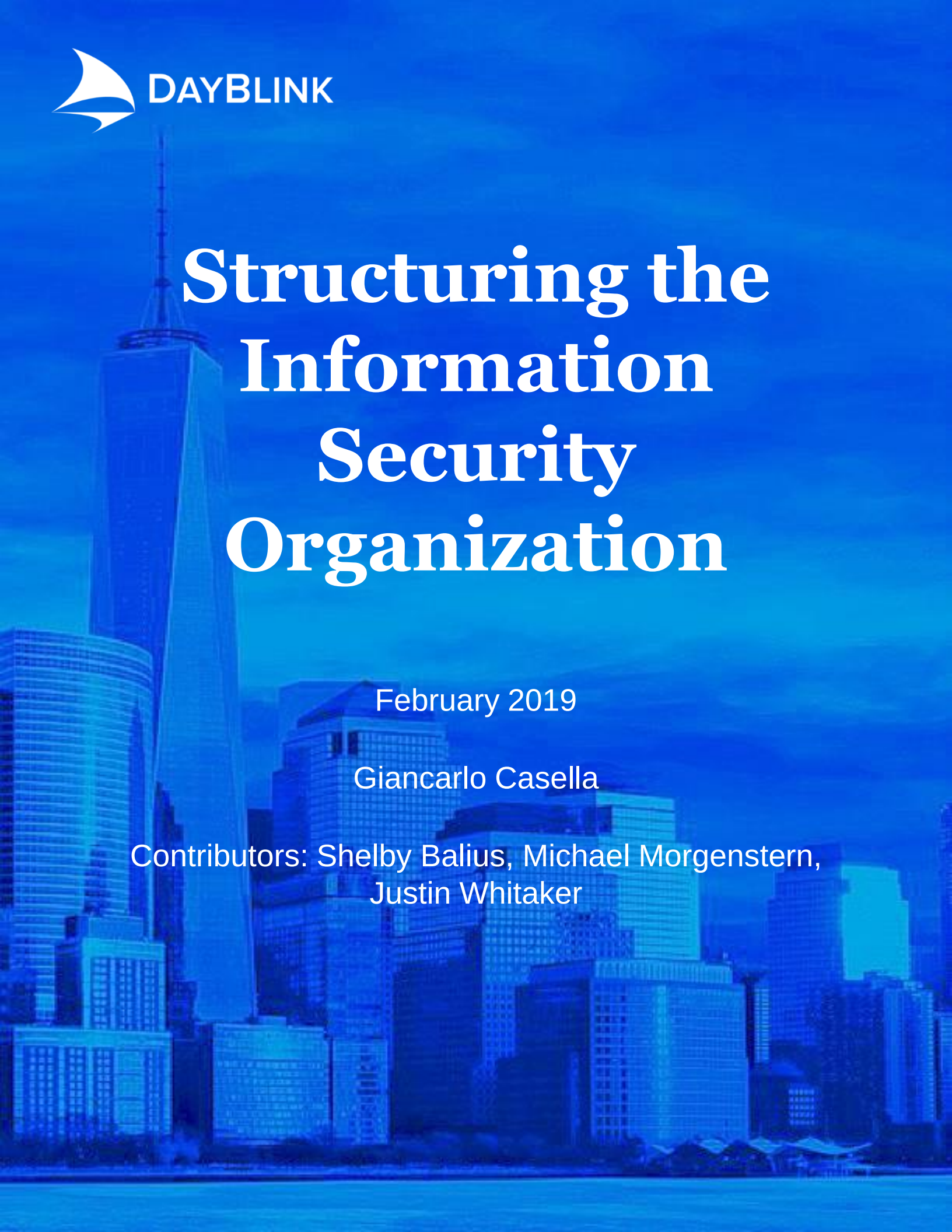


Structuring the Information Security Organization

February 2019

Giancarlo Casella

Contributors: Shelby Balius, Michael Morgenstern, Justin Whitaker

INTRODUCTION

Keeping up with the Evolving Landscape

The continued evolution of enterprise threats has made Chief Information Security Officers (CISOs) consistently seek better opportunities and strategies to defend the perimeter and drive action given scarce resources. Pioneering CISOs capitalize on the opportunity to mitigate threats by optimizing their organizational structure in a manner where defensive and preventative processes are streamlined. Through DayBlink's first hand consultative experience and extensive research, we uncovered a holistic and best-practice organizational structure that identifies and responds to risks consistently and with vigor. In short, our analysis uncovered that there is not a "one-size-fits-all" organizational model that will work for enterprises across industries. There are far too many variables, conflicting priorities, and mandates to identify any one significant model. However, there are several key functions and reporting lines for CISOs to consider in their quest to develop robust and stable organizations.

ORGANIZATIONAL DESIGN

More than Trading Hierarchy for Autonomy

Before designing the right fit for your organization, it is imperative to first build an understanding of the core types of organizational structures. Generally speaking, four common models exist: *Functional, Divisional, Matrix,* and *Flat-archy*. These models fall on a spectrum between two extremes: ***Mechanistic*** (narrow spans of control, high centralization, formalized chain of command, etc.) versus ***Organic*** (wide spans of control, decentralization, loose chain of command).

The selection of an appropriate model is driven by the organization's needs and are often customized by the influence of a company's culture and identity. Several considerations should come into play when designing (or re-organizing) a given structure:

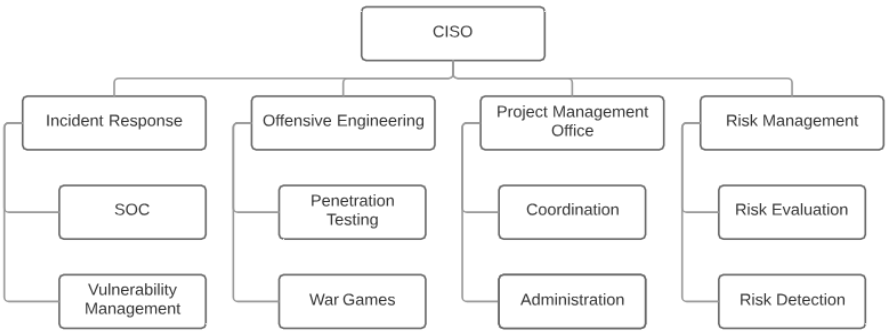
- Which activities are paramount to the CISO organization's integration with the larger enterprise?
- Is there a need for centralized reporting for a company leader or regulator?
- What are the objectives set forth by senior management?
- How can CISO strategies drive enterprise outcomes?
- To what extent are the current resources open to change and transformation?

A brief introduction to the core organizational models is included below.

Organizational Models at a Glance

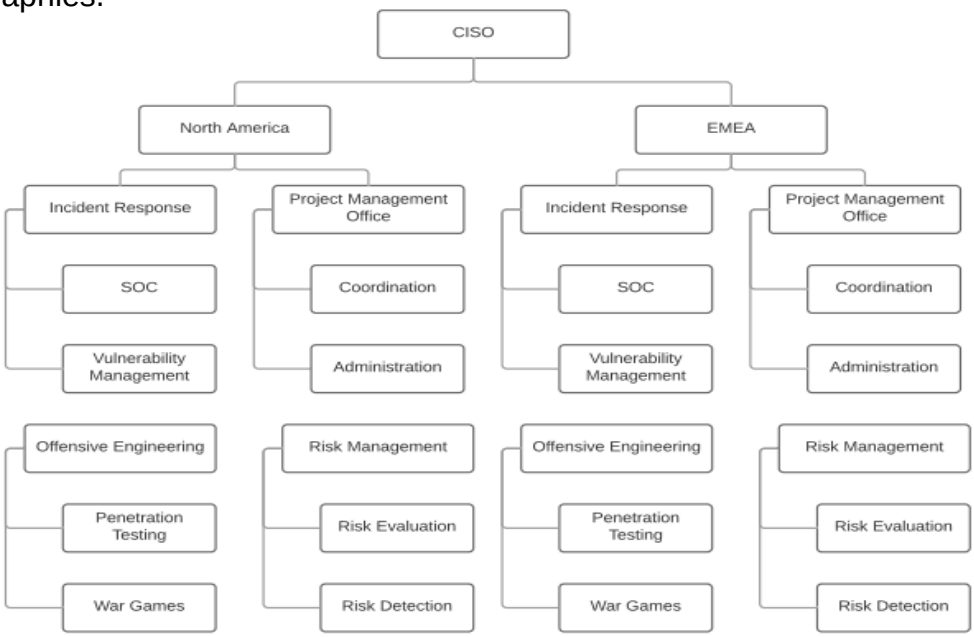
Functional

Functional organizations divide verticals based on specialty or practical operations. This model allows clear roles and responsibilities along with subject matter expertise. A drawback is that this model is prone to silos and lacks cross-specialty collaboration.



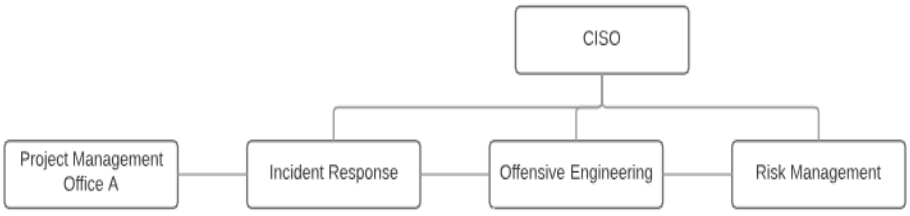
Divisional

Divisional organizations are common across large global enterprises. Due to the scale of some global organizations, cybersecurity responsibilities are defined by geographies. This allows for centralized management among multiple areas but can also perpetuate competing priorities and culture differences between geographies.



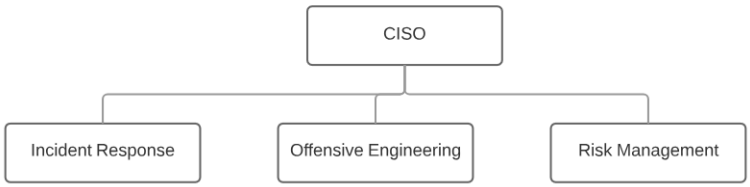
Matrix

In matrix organizations, employees have multiple reporting lines—usually a functional manager, and a project or line manager. Matrix structures allow for flexibility and balanced prioritization but can breed issues with conflicting responsibilities with day-to-day tasks and responsibilities.



Flat-archy

A flat-archy is a model that combines a functional structure with minimal overhead and oversight. A flat-archy allows for quicker and easier decision-making as it groups together resources for their targeted commonalities. Typically, the flat-archy model works well with high potential, well-rounded employees who are able to stretch their usual roles and responsibilities beyond the norm. However, it can cause confusion for employees who are used to "chain-of-command" traditions.



Though we have seen few, select pioneering companies are also starting to experiment with a relatively new type of organizational model called the *Circular Structure* or *Holacracy*. This model focuses on influencing decisions as a group with free flow communication at all levels, collective governance processes to define structure, and individual autonomy in execution. The transformative effort to migrate from a mechanistic structure to this newer style can breed detractors in established organizations, and is more suited for new companies or special ventures.

CISO ORGANIZATIONS

One Size Never Fits All

Throughout our client engagements, we have not seen a dominant type of organizational structure for Information Security organizations. In fact, we have seen all four core models consistently used in varying sizes of enterprises:

The **functional** structure allows for specialty verticals across CISO organizations. Such specialties include Incident Response, Risk Management, and Penetration Testing.

For larger organizations that have global presence, we have seen smaller InfoSec **divisions** with multiple CISOs who span geographies and/or business portfolios with wide-ranging scope.

Certain organizations also employed **matrix** models where, beyond traditional vertical functions, there were horizontal departments such as Project Management Office or Asset Management that managed tasks across verticals.

For younger organizations, we saw more instances of **flat-archy** structures. These “start-up” companies stressed an anti-hierarchical culture where analysts regularly collaborate with senior leadership for projects.

From our experience and analysis, there is not a one-size-fits-all organizational model because each company typically uses a model that positions the firm to its unique competitive advantage. Company culture, senior leadership, and corporate parameters drove the design and execution of each model, ultimately serving the appropriate prioritization of short and long term goals for a given enterprise.

Where Can I Start?

Perhaps you are looking to reorganize the existing CISO organization in your enterprise to better manage threats to the company – or you are tasked with building this competency for your company from the ground up. The core organization models provide a way to organize the people and capabilities. But what people and capabilities should you be seeking?

The “Key Sixteen”

As DayBlink analyzed several in-depth Information Security organizational charts from leading Fortune 50 companies to uncover the common functional threads in successful organizations.

While we did not uncover a predominant organizational structure, there were 16 key functions that the most successful and established organizations had in common:

InfoSec Department	Primary Responsibilities
Blue Team	Oversee all Information Security engineering functions including: Network Security, Software Development, Log Management, Security Architecture, System Administration, and Identity & Access Management
Cyber Crime	Investigate criminal activity that targets infrastructure, consumers, and employees
Identity & Access Management	Process and monitor accounts, roles, identities, and for employees
Incident Response	Detect, analyze and respond to security events and incidents targeting network infrastructure, sensitive data, intellectual property, and employees
Legal	Supervise and oversee the review, negotiation and drafting of major contracts, tender documents and other legal documents and proceedings
Log Management	Log and monitor events across all assets
Network Security	Protect enterprise network environment including network traffic and assets
Project Management Office	Manage high-level projects and maintain Information Security operational functions
Red Team	Identify and exploit security vulnerabilities and study the capabilities of black hat hackers. This function also includes: • Penetration Testing • War Games • Security Product Testing/Evaluation
Risk Management	Identify and manage risk associated with corporate infrastructure and connectivity
Security & Compliance	Track and maintain all reports and actions needed to achieve compliance against security policies, regulations, and audits
Security Architecture	Design, build, and maintain the security structures for networks
Software Development	Create, execute, and maintain software to identify, protect, detect, and respond to attacks
System Administration	Monitor and manage the configuration and operation of network and computer systems
Threat Intelligence	Leverage evidence-based knowledge about an existing or emerging vulnerability to proactively mitigate ramifications
Vulnerability Management & Remediation	Identify, monitor, and remediate vulnerabilities in systems and networks

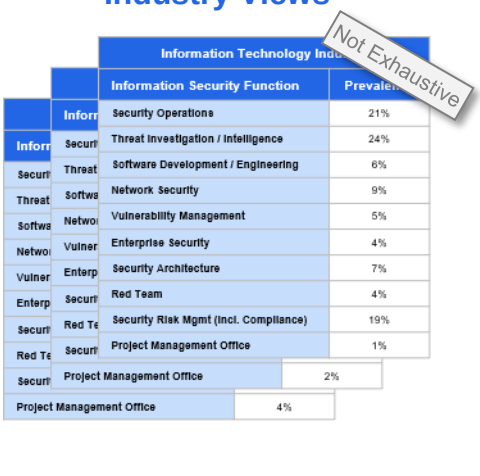
Building the Right Mix of People

DayBlink further analyzed the 16 key functional roles from the previous departments to understand how the human component of the organizations factors into the success of an organization's design. We aggregated average Information Security personnel per function as a percentage of total Information Security personnel. The results are as follows:

Consideration

Senior leadership mandates, business objectives, budgetary constraints, and Information Security maturity drive changes in function prevalence

Industry Views



Aggregated View	
Information Security Function	**Prevalence**
Security Operations	25-30%
Threat Investigation / Intelligence	20-25%
Security Risk Management (incl. Compliance)	15-20%
Network Security	6-12%
Security Architecture	4-5%
Vulnerability Management	2-6%
Software Development / Engineering	1-5%
Enterprise Security	1-3%
Project Management Office	0-5%
Offensive Engineering	0-1%

We observed that indexing the workforce toward a security-focused culture will dictate a consistent personnel distribution in CISO structures – an organization with a security-focused culture will have few managers reporting directly to the CISO. Ideally, there should be a manager for each of the following: Defensive Security/Incident Response – Blue Team, Offensive Security – Red Team, Operations, and Legal & Compliance.

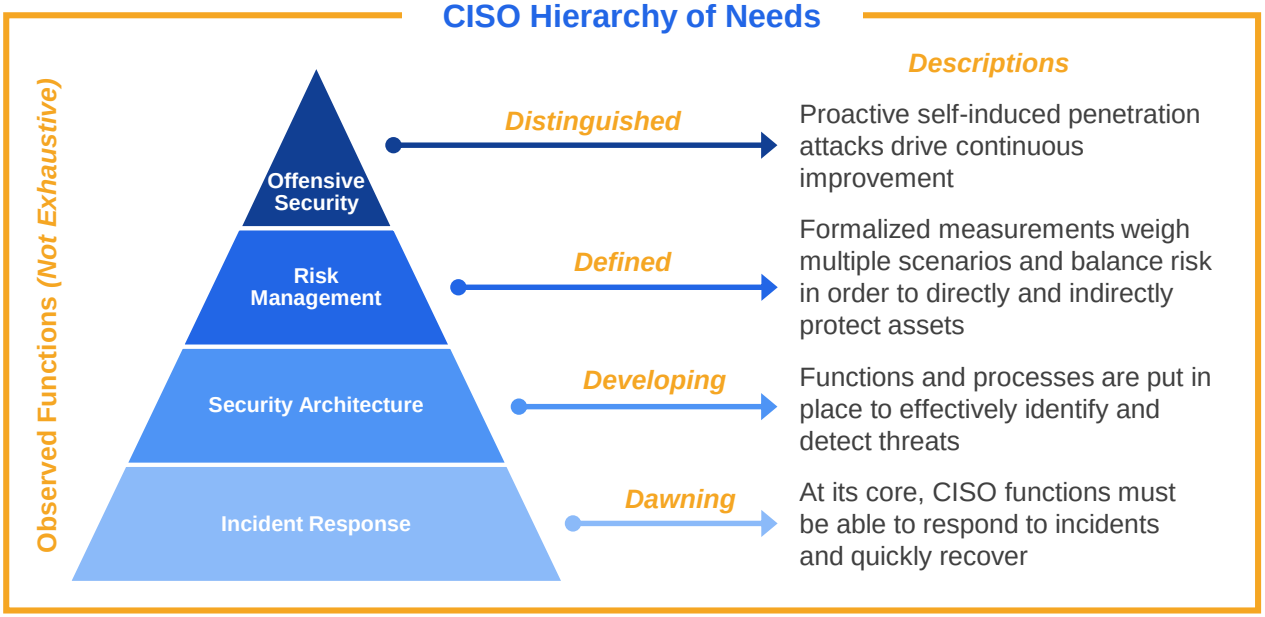
Your C-Suite Matters!

Our observations uncovered an interesting point. At the top level, the CISO should report directly to the CTO, if not directly to the CEO, and the CISO/CIO function should be at the same seniority tranche as each other. Conceptually, CISOs and CIOs are in direct conflict of one another. A CISO's main responsibility is to protect assets while a CIO's main responsibility is to ensure the immediate availability of assets. Security features typically slow down assets, and therein lies the conflict. Both responsibilities are important, but when a CISO reports to a CIO, security will almost always take a seat behind availability. To ensure a just and optimal balance, the CISO and CIO should be peers and report to the same contact, either a CTO or directly to the CEO. Remember this point as a means to further streamline your organization.

CISO HIERARCHY OF NEEDS

Satisfying Basic Needs will Allow for More Sophisticated Processes

Taking into account the commonalities of leading companies as well as the diversity in organization structures across the industry, we created a CISO Hierarchy of Needs, depicted below:



At the minimum, information security organizations must have a dedicated function solely responsible for incident response and recovery. Once these functional needs are satisfied, processes for threat identification and detection are set in place – manifesting as functions such as security architecture, network security, system administration, etc.

With those two foundational needs met, CISOs should begin to expect functions to formally measure risks and potential impacts to assets. This will help the organization proactively mitigate and plan for attacks. At the apex of functional needs, CISOs seek functional teams to self-attack with the use of white and black-box penetration exercises in order to continuously improve their cyber defenses.

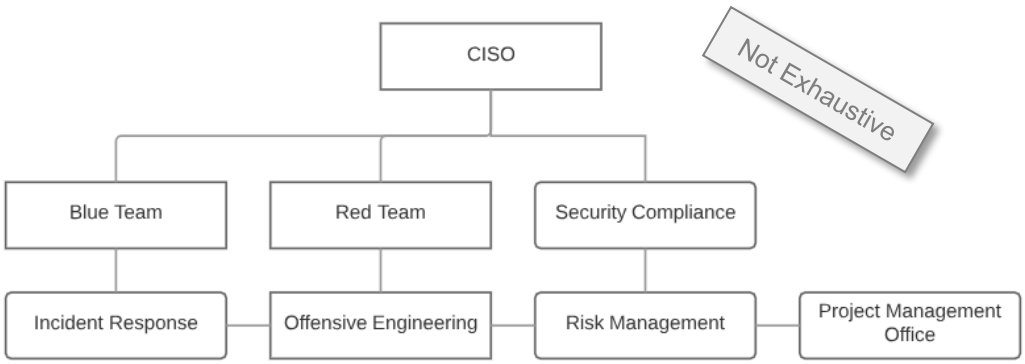
Ultimately, there are many ways to structure your information security organization. Budgetary constraints, senior leadership objectives and mandates will dictate your functional needs which will then influence your organizational structure.

FINAL REMARKS

Ultimately, different organizational models work across industries, and competing priorities and objectives make an “optimal” model an elusive goal. That said, we have uncovered functional commonalities among various CISO organizations, allowing us to create a standardized view of a CISO organization by unifying common functions and processes.

Our view of a CISO organizational structure that is proven to consistently work is one that has three overarching domains with one horizontal: Blue Team, Red Team, Security Compliance, and the Project Management Office (PMO) as the horizontal. **Blue Team** responds, identifies, detects and remediates threats while continually hardening security architectures through software development, etc. **Red Team** tests enterprise defense through penetration testing and war gaming while suggesting areas for improvements based on successful attacks. **Security Compliance** ensures the enterprise is compliant with legal mandates such as HIPAA, GDPR, etc. and models business impact based on a series of risk scenarios. Lastly, positioning the **PMO** as a horizontal allows for careful and impactful project coordination across functions that may naturally be siloed or lack effective communication channels.

This framework has shown to be an exhaustive model that allows for quick and efficient means to mitigate cyber threats and sponsors the alignment of business objectives and senior leadership directives. Based on DayBlink analysis, the organizational structure blueprint below represents a model that has consistently shown to be effective at identifying, protecting, detecting, responding, and recovering from cybersecurity threats.



We assist leading enterprises who are ready to harness the benefits from an organizational redesign that transforms an underperforming or vulnerable organization to one ready to tackle threats head on. A model that leverages three functional domains (Blue Team, Red Team, and Security Compliance) along with a horizontal PMO has proven to be a promising path for success and can help transform an underperforming or vulnerable organization into one ready to tackle threats head on.

ABOUT THE AUTHORS

Giancarlo Casella is a Senior Consultant within DayBlink's Cybersecurity Center of Excellence and is based in the Vienna, Virginia office.

Shelby Balius, PHR® is a Manager at DayBlink specializing in Human Capital and Change Management consulting. She is based in the Vienna, Virginia office.

Michael Morgenstern is a Partner and Practice Lead of DayBlink's Cybersecurity Center of Excellence, a former cybersecurity entrepreneur, and is based in the Vienna, Virginia office.

Justin Whitaker is a Partner and Practice Lead of DayBlink's Cybersecurity Center of Excellence and is based in the Vienna, Virginia office.

ABOUT DAYBLINK

In today's cybersecurity environment, the threat landscape is rapidly evolving. It's outpacing the current defensive resources and skill sets of most corporations – meaning many companies are falling victim to attacks by malicious agents. The way we do business is also changing – with more data stored, living in the cloud, and constantly demand on the go. Breaches can mean losing clients and customers overnight.

DayBlink works with clients to improve their security posture. We assess threats and vulnerabilities, identify organizational risk, prioritize remediation efforts, and implement solutions to secure IT environments and critical assets from sophisticated cyber-attacks.

DAYBLINK

For more information:
Visit: www.dayblink.com/services/technology/cybersecurity
Email: cyber@dayblink.com
Call: 1 (866) 281-4403