The cybersecurity operations center (CSOC) is a vital entity within any enterprise structure. Its responsibilities are dictated by the size of the enterprise, whether the enterprise is multinational, the enterprise’s preference for centralized or decentralized cybersecurity management and operations, and whether the CSOC is in-house or outsourced. In addition, the CSOC mission and charter are highly correlated with how well the enterprise’s executive team understands the intricacies of cybersecurity.

The CSOC is valuable because it combines and maximizes skilled resources, best practices and technology solutions for the purpose of timely detection, real-time monitoring and correcting, and responding to cyberthreats to protect the organization’s assets. In addition, the CSOC has the platform to collect the status of various incidents, infrastructure status and the effectiveness of the enterprise’s defense preparedness through the reporting of predesigned key performance indicator (KPI) metrics intended for various stakeholders. Many factors play a role in establishing and investing in a CSOC. According to a 2019 survey by the SANS Institute, the greatest challenges in establishing a service model for a CSOC are:

- Lack of skilled staff
- Lack of automation and orchestration
- Too many tools that are not integrated
- Lack of management support
- Lack of processes or playbooks

When an enterprise is committed to establishing and investing in a CSOC, these pitfalls must be avoided, and valuable lessons can be learned from other enterprises.

To achieve excellence, KPIs must be identified. KPIs vary from one enterprise to another. Reporting and capitalizing on KPIs is critical to achieve continuous process improvement within the CSOC, which can be the foundation for instituting cultural change within the enterprise.

Functions of a CSOC

The CSOC manages operational cybersecurity activities and identifies, detects, protects against, responds to and recovers from unauthorized activities affecting the enterprise’s digital footprint. The CSOC is dependent on a set of documented processes and procedures, cybertools, and experienced security analysts.
The CSOC is built on three major pillars:
1. Processes and procedures
2. Cyberproducts (e.g., applications and tools)
3. Cyberstaff

The collective performance of these pillars in support of the enterprise is governed by timely threat detection, speed of response and staff competency (figure 1).

For the CSOC to carry out its functions successfully, critical enablers must be in place. The CSOC must protect the entire enterprise, have a clear mission and charter, and be integrated into the business of the enterprise (figure 2).

**What a CSOC Is and Is Not**

The CSOC is not an IT help desk. The major task of an IT help desk is to support the enterprise’s employees. To ensure effectiveness, the enterprise must establish a clear mission and charter for the CSOC and define its functional attributes (figure 3). The CSOC is meant to protect the entire enterprise, and it should be strategically connected to the enterprise’s business objectives. The CSOC must have full access to the enterprise infrastructure, understand critical data classification and be equipped with proven technology solutions.

**Critical Attributes and Challenges: The Top-Down Approach**

A top-down approach to cybersecurity ensures an enterprisewide focus on business objectives. In addition, it ensures that the CSOC will not operate in a silo but will be integrated into all business functions. Identifying the critical attributes of a CSOC is best accomplished with a top-down approach, where the...
mission is aggregated and the charter is based on the goal of best serving the enterprise's objectives and culture. A top-down approach takes a holistic view of the CSOC's critical attributes to accurately reflect cyberenterprise governance. Figure 4 illustrates a method of breaking down each successive layer of the CSOC model into key attributes. The hierarchical structure clarifies the prioritization of each layer, which helps to facilitate decision-making.

The most appropriate approach to constructing a credible CSOC model is through the participation of cross-functional stakeholders in the enterprise.

CSOC execution and daily operations are representative of a bottom-up method. The bottom-up approach ensures that CSOC security requirements are met, best practices are used and full advantage is taken of cyberproducts.

CSOCs in Small, Medium and Large Enterprises

Establishing a CSOC within an enterprise is an expensive endeavor. It requires a substantial capital investment in infrastructure and cyberproducts; the development of policies and procedures; and a commitment to hire, train and retain highly skilled technical analysts. An effective CSOC has to operate 24 hours a day, seven days a week, 365 days a year with staff capable of responding to and thwarting major threats.

As a general rule, enterprise cybersecurity should not be outsourced to a third-party managed security service provider (MSSP). It is ideal for the enterprise to assume substantial responsibility for and have a direct stake in the operational ownership of the CSOC function. Of course, this is based on the enterprise's ability to make the necessary initial investment and commitment to ongoing operational expenditures.

Small enterprises may need to outsource most of the CSOC functions to an MSSP. Medium-size enterprises often build various CSOC capabilities into their own cybersecurity functions and outsource a few other CSOC functions to third parties to mitigate the costs. For example, midsize enterprises may consider outsourcing penetration testing, vulnerability scanning, security assessment and employees’ cybertraining. Another possibility for outsourcing is second- or third-shift incident monitoring and reporting with temporary cyber fixes while the core CSOC team is operating in the first shift.

An effective CSOC assumes control of the operation and management of the enterprise's security monitoring, cyberprotection, cyberremediation and cyberreporting of KPIs. There should be a set of applications and tools supporting the identification, detection, protection against and response to cyberthreats and the recovery of

<table>
<thead>
<tr>
<th>Critical Attributes of Effectiveness</th>
<th>Enterprise-level function</th>
<th>Integrated with the business objective of the enterprise</th>
<th>Has the focus of the BoD</th>
<th>Has full visibility of the enterprise's digital infrastructure</th>
<th>Inclusive in cybersecurity jurisdiction</th>
<th>Equipped with competent staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical Attributes of Functional Responsibilities</td>
<td>Real-time monitoring</td>
<td>Incident validation</td>
<td>Threat containment and eradication</td>
<td>KPIs and dashboard reporting</td>
<td>Continuous process improvement</td>
<td>Maximized automation</td>
</tr>
<tr>
<td>Critical Attributes of Challenges</td>
<td>Operates as an IT help desk</td>
<td>Unsuitability with the enterprise culture</td>
<td>Operates in isolation</td>
<td>Insufficient funding</td>
<td>Unable to capture and quantify success</td>
<td>Outsourcing critical functions</td>
</tr>
</tbody>
</table>

Figure 4—CSOC Critical Attributes

"THE MOST APPROPRIATE APPROACH TO CONSTRUCTING A CREDIBLE CSOC MODEL IS THROUGH THE PARTICIPATION OF CROSS-FUNCTIONAL STAKEHOLDERS IN THE ENTERPRISE."
business operations after an event. In addition, it is critical for the CSOC to report its KPIs in compliance with standards and frameworks such as the International Organization for Standardization (ISO) ISO 27001/27002, the US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, the Payment Card Industry Data Security Standard (PCI DSS), the US Federal Financial Institutions Examination Council (FFIEC), and the US Health Insurance Portability and Accountability Act (HIPAA). The scope of CSOC reporting and monitoring includes, but is not limited to, the following:

- Network and server firewalls
- Configuration management
- Incident management
- Server and endpoint antivirus protection
- Web application firewalls
- Two-factor authentication (2FA)
- Identity management
- Security information and event monitoring (SIEM)
- Database monitoring
- Whitelisting
- Blacklisting
- Network anomaly detection
- Email antispam protection
- Email antimalware protection
- Email antispoofing protection
- Validation of vulnerabilities
- Patch management
- Data leakage protection
- Encryption
- File integrity monitoring
- System backups

**Selecting CSOC Building Blocks**

Reverse engineering can be used, based on predefined KPIs, prior to committing to the development of policies and procedures, the selection of cybertools, and the hiring and training of employees. Reverse engineering enables the enterprise to identify the necessary components of a CSOC based on expected outcomes of reported indices in direct support of enterprise objectives. The CSOC management team should always complete the following steps:

- List which KPIs to report, and then identify the processes and procedures, technology solutions, and staff skills that are required. Examples of CSOC KPIs are number of incidents, categorization of incidents based on significance, time from discovery to containment to eradication of threats, length of time employee or contractor credentials stay active after termination of employment, frequency of validation of active employees by line of business, tracking of who is granted access to enterprise systems, and role-based access.

- Develop processes and procedures that cyberanalysts will be required to follow when faced with different cyberthreat scenarios. This should be the foundation of cybertraining, and it will ensure consistency throughout the enterprise.

- Identify where cyberapplications and cybertools fit within the enterprise’s digital blueprint and which functions they will perform. Examples include endpoint protection, firewalls, SIEM, virus and malware protection, security monitoring applications, and patch management. The key is to build standard operating procedures (SOPs) for the staff to follow in response to various threats using the implemented cybertechnology applications and tools.

“SETTING UP AND INVESTING IN A NEW CSOC IS A MAJOR COMMITMENT, REGARDLESS OF THE SIZE OF THE ENTERPRISE.”

**Pitfalls to Avoid**

Setting up and investing in a new CSOC is a major commitment, regardless of the size of the enterprise. It must be planned, designed and managed prudently. It is critical to build effective and efficient CSOC performance into its core governance through effective planning, sound investment, management of skilled resources, documented processes and procedures, and well-
designed infrastructure to protect the enterprise from cybersecurity risk.

It is unwise to try to design an airplane while flying it; it will crash. Similarly, enterprise management can avert a crash by avoiding the following pitfalls when instituting and operating a CSOC:

- Never assume that there is a 100 percent secure environment. Successful security operations are possible only when enterprises continually improve their cybersecurity functions with frequent updates. It is important to prioritize assets, isolate high-value asset networks, tighten internal controls, implement real-time monitoring and alerts, and perform frequent audits.

- Do not outsource the entire CSOC. Doing so amounts to outsourcing all responsibility for enterprise security. Accountability cannot be outsourced; it is owned by the enterprise itself. Partial outsourcing of a few CSOC functions is acceptable, but critical CSOC functions should remain in-house to the extent possible.

- Trying to secure everything means securing nothing. Every day brings new cyberthreats in the form of ransomware, malware, phishing, social engineering and data breaches. Investing in cybersecurity teams, tools and applications is not the absolute answer. A balance must be struck among investing in employee training, cybertools and policies, and procedures to ensure that the enterprise is in an optimal position to respond to cyberthreats.

- Technology cannot replace people. Artificial intelligence (AI) applications are not a substitute for human intelligence. Practically speaking, AI in cybersecurity is not yet sufficiently mature. Replacing people with technology will relinquish the human side of the enterprise’s environment, culture and business. Currently, enterprises should rely on qualified staff to validate and apply corrective actions.

- Using too many cyberproducts can crowd the technology ecosystem and lead to conflicting products. Avoid redundancy in cybertechnology functions, simplify the cyberapplication architecture and prioritize the digital architecture.

- Fixing incidents after they occur is not sufficient to establish a sense of cybersecurity. Security analysts should be trained to identify the root causes of problems and eradicate them. KPIs should capture trends in cyberthreats (e.g., by identifying 12-month rolling trends).

- There is no simple answer to centralized vs. decentralized planning and execution. It depends on the size of the enterprise. Decision-making is an art, not a science. There is no mathematical equation that will yield exact quantitative results. Creative thinking and competent management are needed to determine the appropriate degree of centralization and decentralization of the CSOC’s governance, planning and execution.

- One team or one resource cannot do it all. The CSOC will be most effective when there are specialized teams and segregation of duties. There should be various teams focusing on real-time monitoring and reporting; incident validation, containment and eradication; centralized reporting and dashboarding of KPIs; and continuous process and technology improvement (Figure 5).

- Do not be caught without a playbook for handling cyberincidents. An incident response playbook should be compiled beforehand to the extent possible. CSOC processes should be documented and disseminated, and systems analysts should be trained to follow appropriate procedures.

“SETTING UP AND INVESTING IN A NEW CSOC IS A MAJOR COMMITMENT, REGARDLESS OF THE SIZE OF THE ENTERPRISE.”
The CSOC cannot operate in a vacuum. Its effectiveness stems from receiving input from and collaborating with various stakeholders such as the chief information security officer (CISO), IT, the IT help desk, the end user community, solution providers and industry consortia (Figure 6).

**Key Reporting and Performance Indicators**

KPIs are used to measure, track and report actual achievements vs. targets. KPIs for the CSOC serve multiple purposes, such as measuring its operational effectiveness and efficiency, identifying internal control gaps and required remediation, and justifying capital investment and operational budgets.

The CSOC is well positioned to report KPIs of value that are actionable by the cybersecurity team to the enterprise through established processes, tools and staff. The most valuable KPIs are those connected to the enterprise’s objectives and easily understood by the nontechnical senior management team. Actionable KPIs are related to key internal controls where gaps can be identified and remediation can be planned. KPIs are subject to frequent security assessment and cybersecurity process improvement. They can serve as the metrics to determine a business unit’s risk and the impact on a particular department.

**Dashboard Illustration**

Enterprises determine which KPIs to use and track and how to report them. However, KPIs are expected to evolve over time as CSOC operations mature, the business changes or new cyberthreats emerge.

Dashboard reporting enables the audience—both technical and nontechnical—to understand the “as is” status and identify the desirable “to be” state. In other words, dashboarding is a useful communication tool for interpreting the operational efficiency of the current cyberstate and the efficacy and effectiveness of the CSOC processes, procedures and team in detecting, containing and eradicating cyberthreats. In addition, it can help the enterprise scrutinize the design and operational effectiveness of the key controls and how the enterprise measures up against its peers. Dashboarding enables management to narrow its focus and drill down to the lowest entity among its groups and controls.

The KPI dashboard shown in Figure 7 uses color coding to denote the following:

- **Blue**—Exceeds KPI target
- **Green**—Satisfies KPI target
- **Orange**—Below KPI target and requires attention
- **Red**—Seriously below KPI target and requires immediate remediation

A rolling 12-month trend report is valuable to track security incidents and CSOC operational progress (Figure 8). These trends include:

- Number of alerts
- Number of false positives

---

**Figure 6—Input/Output, Interface and Communication**

- **End Users**
- **CISO**
- **Solutions Providers**
- **IT and IT Help Desk**

---

<table>
<thead>
<tr>
<th>Process Improvement</th>
<th>Real-Time Monitoring/Communication</th>
<th>Incident Validation</th>
<th>CSOC</th>
<th>KPIs Dashboard Reporting</th>
<th>Containment and Eradication</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---
Figure 7—KPIs: CSOC Monthly Dashboard

<table>
<thead>
<tr>
<th>KPI</th>
<th>Target</th>
<th>Actual</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.T. KPI: Mean Time to Contact (MTC)</td>
<td>Target</td>
<td>Actual</td>
</tr>
<tr>
<td>EQ KPI: Mean Time to Detect (MTD)</td>
<td>Target</td>
<td>Actual</td>
</tr>
<tr>
<td>L.T. KPI: Mean Time to Eradicate (MTE)</td>
<td>Target</td>
<td>Actual</td>
</tr>
<tr>
<td>Failed KPI: Mean Time to Investigate (MTI)</td>
<td>Target</td>
<td>Actual</td>
</tr>
<tr>
<td>EQ KPI: Days Deactivated Ex-Employee</td>
<td>Target</td>
<td>Actual</td>
</tr>
<tr>
<td>L.T. KPI: Frequency Review of 3rd Parties</td>
<td>Target</td>
<td>Actual</td>
</tr>
<tr>
<td>L.T. KPI: Frequency Review of Active Directory</td>
<td>Target</td>
<td>Actual</td>
</tr>
<tr>
<td>Failed KPI: Frequency Review of Cyber Policies</td>
<td>Target</td>
<td>Actual</td>
</tr>
</tbody>
</table>

Figure 8—KPIs: 12-Month Rolling Trends

- Number of reported incidents
- Number of devices monitored
- Number of superusers

“Go to Green”: From KPIs to Process Improvement to Remediation

The journey to CSOC process improvement starts with the KPI report. The KPI dashboard highlights the strengths and weaknesses of the CSOC and the enterprise's cyberoperation as a whole by business units, key internal controls and by other measures. This triggers the initiation of a risk assessment for a particular digital footprint of the enterprise or functional area. The findings and conclusions of the risk assessment establish the foundation for the development of a remediation plan, triggering a process improvement initiative. In addition, this can be used to establish management approval and budget allocations for such endeavors.

Adopting the “go to green” process (figure 9) will instill a culture of transformation and indoctrination of the CSOC, serving the goal of continuous improvement.
Figure 9—Go to Green Process Flow

KPIs-CSOC Monthly Dashboard Month of MM/YYYY

<table>
<thead>
<tr>
<th>KPI</th>
<th>Description</th>
<th>Target</th>
<th>Actual</th>
</tr>
</thead>
<tbody>
<tr>
<td>EQ</td>
<td>Mean Time to Detect (MTD)</td>
<td>Target</td>
<td>Actual</td>
</tr>
<tr>
<td>EQ</td>
<td>Mean Time to Contact (MTC)</td>
<td>Target</td>
<td>Actual</td>
</tr>
<tr>
<td>L.T.</td>
<td>Mean Time to Eradicate (MTE)</td>
<td>Target</td>
<td>Actual</td>
</tr>
<tr>
<td>Failed</td>
<td>Mean Time to Investigate (MTI)</td>
<td>Target</td>
<td>Actual</td>
</tr>
</tbody>
</table>

EQ KPI: Days Deactivated Ex-Employee

KPIs-CSOC Security Risk Assessment

Key Processes | Impact (0-6) | Likelihood (0-5) | Risk = Impact / Likelihood

1. Personnel Security
2. Physical Security
3. Account and password management
4. Confidentiality of sensitive data
5. Disaster recovery
6. Security awareness and education
7. Compliance and audit
8. Information security incident management
9. Business continuity management
10. Information security policy (InfoSec)

Remediation Immediate +3 months +6 months +9 months +12 months

Conclusion

In the current business environment, enterprises’ CSOC functions might range from simple to sophisticated, depending on the size of the enterprise, the nature of the business, the organizational culture and the willingness to invest. This determines whether the enterprise outsources the CSOC to a third-party MSSP, retains most CSOC functions in-house, or implements a combination of insourcing and outsourcing.

The CSOC is not an IT help desk. It is a vital entity that supports the entire enterprise. It is an integral part of the business that collaborates with cross-functional stakeholders. Because the CSOC provides vital functions, its critical attributes must be maintained, and challenges and pitfalls must be avoided.

KPIs should be identified and integrated in a management dashboard that is easy for both technical and nontechnical staff to understand. KPIs and the management dashboard enable the CSOC to focus on the root causes of problems, leading to continuous improvement of the enterprise’s cyberposture.

Endnotes