WHY YOU NEED A VIRTUAL CHIEF SECURITY OFFICER, OR vCSO

Our Virtual Chief Security Officer (vCSO) solution will help your business make security decisions, understand security threats, and optimize security processes. With our vCSO solution, you will retain a board-level resource who can virtually sit inside your company and manage your security strategy, budget, review of risks and regulatory programs.

GET THE BENEFIT OF HIGHLY-SPECIALIZED SECURITY TALENT FOR A FRACTION OF THE COST OF A FULL-TIME STAFF MEMBER

Threat Intelligence
Provides context for decisions being made within the cybersecurity program

Risk Analysis
Prioritizes items for completion within the organization —provides a trustworthy place to start

Security Accountability
Creates oversight for the organization's security —the Executive team knows it is being proactively managed

Board-level Discussion
Communicate business security risk and outcomes to the board, now that it is a board-level expectation

IT Meets IS
Someone on the team focused on making sure it gets done in a secure matter – not just done

Scope of Cybersecurity Activity:

- Threat Modeling
- Risk Management
- 3rd Party Pen Testing
- Regulatory Compliance
- System Patching
- Security Architecture
- Data Protection

With our vCSO solution, we will not be sitting on the sidelines.
Our goal is to be constantly and consistently delivering you results. Below we will outline the ongoing items that we will be providing as apart of this solution.

WEEKLY:

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52	**IT Status Meeting** *(Optional)* Attend IT Status Meeting to provide updates on projects, answer tactical security questions, and get decisions from leadership as needed; review any current security vulnerabilities and discuss how the organization may or may not be impacted.

MONTHLY:

J F M A M J J A S O N D	**IT Performance Analysis** Audit monthly IT activities, document findings and initiate/request/validate any necessary changes.
J F M A M J J A S O N D	**IT Security Meeting** Meeting to review issue progress, vulnerability test results, security project status, plan for upcoming events, and review/edit deliverables as needed.
J F M A M J J A S O N D	**Simulated phishing exercises*** Deploy simulated phishing exercises and analyze results for frequent clickers or other signs and/or anomalies (*Requires investment in advanced security stack)
J F M A M J J A S O N D	**Back-up Review** Review back-up of all endpoint machines and servers to ensure that they are occurring on a timely basis and are within backup service level agreement.

QUARTERLY:

Q1 Q2 Q3 Q4	**User Privilege Review** Review the list of Line of business, M365 and domain users to ensure no unneeded users; verify tickets were created for user termination requests as well as any Human Resources changes.
Q1 Q2 Q3 Q4	**Executive Leadership Meeting** Meet with executive team (CEO, COO, CFO, GC and CAO) to provide updates on current trends in IT security, latest vulnerability analysis and status of IT projects; supplement with further updates as needed.
Q1 Q2 Q3 Q4	**IT Security Training** Select and initiate IT security training to all endpoint users through the Galactic portal.
Q1 Q2 Q3 Q4	**Vulnerability Scan/Security Analysis** Provide ongoing security analysis of network, provide/review report findings with leadership and assist in necessary remediation projects.

BI-ANNUALLY:

1 2	**Board Update Meeting** Prepare and present updates for Bi-Annual Cyber Security Risk Board Update. Prior to update confirm content with executive team and review discussion topics.

ANNUALLY:

◯	**Physical Inventory Review** Review the list of IT equipment to ensure it is up to date and all assets are accounted for.
◯	**Third-Party Penetration Testing** Schedule, coordinate and oversee third-party penetration testing; coordinate and remediate any findings from the testing.
◯	**Policy Review** Review policies and make updates based on organizational changes; if changes are made to acceptable use policy, coordinate with legal and incorporate into Employee Handbook as needed; create and implement new policies as needed.
◯	**Procedure Review** Review and update procedures
◯	**Vendor Review** Conduct security review of vendors, including completion of Vendor Self-Assessment Questionnaires; initiate/oversee vendor security changes as needed; Review most current contract to determine if updates are needed.
◯	**Risk Assessment** Review the different types of risk facing the business units; prioritize security and compliance investments and initiatives based on risk findings.
◯	**PCI Self-Assessment** Complete and save to file the annual self-assessment questionnaires for compliance purposes.
◯	**Tabletop Exercise** Perform annual table-top exercise of the disaster recovery plan/incident response plan with applicable IT vendors and company personnel.
◯	**Inventory Data Assets** Review the list of assets/vendors with the executive team on an annual basis, generally as part of quarterly IT executive meeting; review list of Key Vendors in IT security portal to ensure it is up to date.

AS-NEEDED:

Site Visits: Conduct in-person visits to organization's sites to review on-site security practices and initiate necessary changes.

Threat Intelligence Emails: Provide threat intelligence emails to organization as relevant.

Audit Representation: Proper C-level representation in the event of a formal audit

Security Deliverables: Provide other security deliverables and best practices as needed.