


TECHELLENCE CHIEF SECURITY OFFICER

**MAKE INFORMED SECURITY DECISIONS,
UNDERSTAND SECURITY THREATS, AND
OPTIMIZE SECURITY PROCESSES**



ABOUT TECHELLENCE

Techelligence is a premier technology solutions provider that empowers businesses to thrive with minimal or no internal IT staff. Our expert team delivers comprehensive infrastructure setup, systems management (managed services), software development, and automation, enabling your business to leverage technology as a powerful catalyst for growth. At Techelligence, we are dedicated to enhancing your profitability, efficiency, and security, ensuring that technology becomes a driving force behind your success.

 (844) 832-4244

 techelligence.com

CORPORATE-LEVEL SECURITY ADVISOR AT YOUR SERVICE

With Techelligence Chief Security Officer (CSO) at your side, 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 a 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

Information Technology Meets Information Security

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 Chief Security Officer solution, see transformative changes.

We will consistently deliver results for you. Below outlines the ongoing items to be provided as a part of this solution.

MONTHLY

IT Performance Analysis

Audit monthly IT activities, document findings and initiate/request/validate any necessary changes.

IT Security Meeting

Meeting to review issue progress, vulnerability test results, security project status, plan for upcoming events, and review/edit deliverables as needed.

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)

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

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.

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.

IT Security Training

Select and initiate IT security training to all endpoint users.

Vulnerability Scan/Security Analysis

Provide ongoing security analysis of network, provide/review report findings with leadership and assist in necessary remediation projects.

BI-ANNUALLY

Board Update Meeting

Prepare and present updates for Bi-Annual Cyber Security Risk Board. Confirm content with executive team and review discussions prior.

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 current contracts 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, 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.



 sang@techellence.com

 (844) 832-4244

 techellence.com

 250 Pehle Ave, Suite 200
Saddle Brook, NJ 07663