**Gregory C. Thompson MBA, MPA, MS-Cybersecurity**

Dunn Loring, VA 22027 | 571-488-7247 | gregthompson\_27@yahoo.com | [LinkedIn URL](https://www.linkedin.com/in/gthompson327/)

**CHIEF SECURITY OFFICER | CHIEF INFORMATION SECURITY OFFICER | VP, PHYSICAL SECURITY | VP, INFORMATION SECURITY**

**Empowering organizations to navigate today’s complex threat landscape with visionary leadership and innovative security solutions.**

Dynamic and results-driven Security Executive with a proven track record of leading comprehensive security strategies across physical, personnel, and information domains to safeguard assets, operations, and reputation. Expertise in designing, implementing, and optimizing strategic security programs that align with organizational goals, ensuring regulatory compliance and operational excellence. Recognized for driving transformative process improvements, spearheading change management initiatives, and executing high-stakes projects in complex environments. Adept at building and leading high-performance teams, fostering collaboration, and deploying advanced security protocols to mitigate risks, protect critical infrastructure, and enhance organizational resilience. Known for a proactive, solutions-oriented approach to addressing security challenges and ensuring the safety of personnel, equipment, and information at all levels.

**Core Competencies:**

Investigations | Lean Methodologies | Business Analysis |Conflict Resolution | Compliance Network Security | Strategic Planning | Complex Problem-Solving | Program Management | Emergency Management | Threat Assessment & Mitigation | Leadership Operations | Security Development & Management | Cybersecurity Strategy Development | Governance, Risk & Compliance (GRC) | Crisis & Incident Management |Physical Security Management| Threat intelligence and Analysis | Security Architecture & Design | Security Audits & Compliance | Data Privacy and Protection | Security Program Development & Implementation | Employee & Personnel Security | Leadership & Team Building | Stakeholder Management & Reporting | Budget & Cost Optimization for Security Programs | Regulatory Compliance | Physical & IT Security Convergence | Advanced Threat Detection & Response | Zero Trust Architecture | Security Training & Awareness Programs | Digital Forensics & Incident Response | Security Policy & Procedure Development

**Strengths & Value Offered**

* Proactively developed and implemented comprehensive Business Continuity Plans (BCPs) to safeguard organizational operations during crises, leveraging a systematic approach to identify critical activities, allocate essential resources, and ensure seamless communication with stakeholders. Resulted in minimized operational downtime, enhanced employee support, and the preservation of organizational reputation.
* Demonstrated exceptional leadership by setting high-performance standards and fostering a culture of accountability and collaboration, addressing challenges head-on, and inspiring teams to exceed expectations. Enhanced productivity and morale, driving successful execution of organizational initiatives.
* Conducted in-depth physical security risk assessments to identify vulnerabilities and recommended actionable improvements to senior management. Implemented targeted process enhancements that significantly mitigated risks, ensuring the safety of assets, personnel, and operations.
* Managed critical security operations for the Federal Bureau of Investigation, holding an active Top Secret (TS) Security Clearance and overseeing physical, personnel, and cybersecurity functions. Maintained rigorous compliance with national security protocols, protecting sensitive information and infrastructure.
* Possess exceptional interpersonal, communication, and presentation skills, effectively engaging with diverse populations across all organizational levels. Known for translating complex security concepts into actionable strategies, ensuring alignment and buy-in from stakeholders.

**PROFESSIONAL EXPERIENCE**

**Vantage Data Centers Sterling, VA *Chief Information Security Office* 2022-2025**

*Dynamic and results-driven Chief Information Security Officer (CISO) with a proven track record of architecting and executing enterprise-wide cybersecurity strategies, risk management frameworks, and compliance initiatives that protect critical assets and drive business success. Adept at collaborating with C-suite executives and board members, building high-performing teams, and delivering measurable results aligned with organizational objectives. Recognized for transforming security operations, mitigating risks, and enhancing organizational resilience in complex, high-stakes environments.*

* Automated security reporting processes, reducing reporting time by 50% and improving accuracy for executive-level presentations.
* Designed and implemented a comprehensive enterprise cybersecurity strategy, reducing organizational risk by 35% through advanced threat intelligence, vulnerability management, and robust incident response protocols.
* Developed and operationalized a scalable risk management framework, ensuring compliance with GDPR, HIPAA, and PCI DSS while aligning cybersecurity objectives with business goals via NIST CSF, ISO 27001, and CIS benchmarks.
* Directed audits, penetration tests, and remediation initiatives, achieving a 98% reduction in compliance-related vulnerabilities over two years and ensuring regulatory readiness.
* Spearheaded response efforts for high-profile security incidents, including ransomware attacks and advanced persistent threats (APTs), mitigating financial impact and restoring operations with minimal disruption.
* Built and led the Incident Response Team (IRT), formalizing playbooks, conducting tabletop exercises, and enhancing readiness to handle evolving threat landscapes.
* Transformed cloud security infrastructure, leading the migration to secure cloud platforms by integrating multi-factor authentication (MFA), CASB solutions, and encryption technologies, achieving a 99.9% SLA uptime.
* Implemented Zero Trust Architecture with advanced EDR, identity governance, and micro-segmentation, fortifying the organization’s defense against insider and external threats.
* Scaled and optimized the global cybersecurity team by 40%, fostering a culture of excellence and mentoring emerging leaders, resulting in a 25% promotion rate.
* Negotiated and managed vendor contracts, achieving a 20% cost reduction while maintaining high service quality and ensuring cutting-edge security solutions.
* Established a Data Loss Prevention (DLP) program, decreasing incidents of sensitive data exfiltration by 40% and improving data security policies in collaboration with legal and compliance teams.
* Presented strategic cybersecurity updates to board members and executive teams, delivering actionable insights into the organization’s risk posture through well-defined KPIs and security metrics.
* Automated reporting processes, reducing reporting time by 50% and enhancing the accuracy of executive-level presentations.

**Vantage Data Centers Sterling, VA *Vice President, Physical Security & Cybersecurity* 2019 - 2022**

*Directed and managed comprehensive security operations across seven geographically dispersed data centers (DCs) spanning three North American time zones. Delivered seamless integration of IT and physical security while fostering a culture of excellence, compliance, and continuous improvement. Recognized for driving operational efficiency, reducing costs, and enhancing the security posture of critical infrastructure.*

* Led and developed a high-performing team of supervisors and guards, overseeing daily operations, training, and compliance across multiple data center locations. Unified operational procedures and streamlined reporting structures, reducing overtime costs by 23%.
* Designed, implemented, and managed a comprehensive staffing plan for all physical security vendors, ensuring optimal hiring, training, supervision, and compliance with regulatory and organizational standards.
* Improved operational efficiency and reduced security officer turnover by 5.7%, while decreasing key performance metrics, including incident rates and alarm response times, by rebidding and standardizing vendor contracts.
* Directed all aspects of customer safety requirements, including IT/physical security interface, site design, construction, testing, daily operations, and maintenance. Achieved measurable cost efficiencies by collaborating with finance and construction teams to track the effectiveness of security budgets and build metrics.
* Fostered a metrics-driven culture of continuous improvement, partnering with the Performance Optimization team to implement industry best practices, resulting in enhanced site security and operational consistency.
* Identified and mitigated existing and emerging risks, ensuring business activities adhered to robust risk management frameworks and addressing cyber vulnerabilities through proactive response efforts.
* Spearheaded the design, development, and deployment of advanced cybersecurity solutions, leading the Cyber Security Engineering team in delivering prevention, detection, and response capabilities. Enhanced resilience through comprehensive digital forensics and vulnerability management programs.
* Developed and implemented global security frameworks, achieving compliance with ISO 27001, NIST 800.53, and ISA 95. Continuously evaluated and updated security strategies to stay ahead of evolving threats.
* Collaborated with law enforcement agencies to address major cyber incidents, ensuring timely response and resolution of vulnerabilities while minimizing business disruptions.

**General Dynamics Corporate Falls Church, VA *Senior Security Manager/Facility Security Officer* 2013-2019**

*Directed industrial, physical, and information security operations for over 400 employees, ensuring compliance with regulatory standards, client contracts, and company policies. Managed personnel clearances, employee briefings, visit requests, and the administration of the National Industrial Security Program Operating Manual (NISPOM). Oversaw compliance programs by addressing regulatory concerns, resolving issues, and implementing solutions. Prepared for and successfully completed government audits and inspections, maintaining high standards of regulatory adherence and operational effectiveness.*

* Supervised and implemented enterprise-wide security protocols, including the administration of the National Industrial Security Program Operating Manual (NISPOM) and compliance with evolving security regulations, resulting in the successful completion of audits and government inspections.
* Served as a Subject Matter Expert (SME) for business continuity planning, workplace violence prevention, crisis management planning, facility security awareness, counterintelligence for foreign travel, and the Global Response Center.
* Optimized the department's $4.7M budget, identifying cost-saving initiatives and maintaining projects within scope, enabling the strategic upgrade of security equipment across five facilities while enhancing operational efficiency.
* Designed and executed robust compliance programs, collaborating with cross-functional teams to establish effective policies and procedures, resolve compliance issues, and investigate potential violations to ensure regulatory adherence.
* Enhanced communication security across remote sites by conducting risk assessments, identifying vulnerabilities, and overseeing the design and implementation of secure communication networks to protect sensitive data.
* Led employee security clearances, briefings, and visit requests, ensuring personnel were informed of and compliant with organizational and regulatory security standards.
* Improved organizational readiness and response capabilities by delivering facility security awareness and training programs tailored to employee roles, contributing to a culture of vigilance and accountability.

**Federal Bureau of Investigation (FBI) Washington, DC *Personnel Security, Acting Associate Chief Security Officer* 2011-2013**

*Ensured a safe and secure environment for a facility of over 400 employees by overseeing physical and personnel security measures. Directed security strategies and initiatives across multiple business units to align with organizational objectives. Provided governance and accountability for risk and controls management, policy and program management, security incident management, security monitoring, threat, and intelligence, and vulnerability assessments. Conducted monthly audits to identify potential security issues, inspected designs and installations for regulatory compliance, and implemented best practices to mitigate risks and enhance operational efficiency.*

* Delivered security awareness training to promote employee understanding of critical security measures.
* Streamlined a contractor management program by implementing an organized filing system, significantly reducing administrative overhead.
* Conducted physical security risk assessments, presented actionable recommendations, and implemented process improvements that reduced organizational risk.
* Enhanced security programs and procedures to ensure employee safety, including initiatives for foreign travel, visitor protocols, DOE clearances, and polygraph programs.

**Federal Bureau of Investigation (FBI) Washington, DC**

***Personnel Security Specialist* 2009-2011**

*Managed the full lifecycle of security clearance processes for government employees and applicants, from screening and evaluation to final adjudication. Conducted thorough risk assessments and reviewed personnel backgrounds to ensure compliance with federal regulations, specifically those set by the Department of Defense (DoD) and Intelligence Community (IC). Used policies and procedures from the federal government, including Executive Orders, to ensure the accurate and timely processing of clearance requests. Worked closely with various departments to ensure all required personnel security questionnaires were reviewed, processed, and approved within compliance standards. Identified gaps in existing processes and developed improvements to enhance productivity, streamline operations, and maintain a high level of accuracy in personnel clearance procedures.*

* Utilized advanced skills in adjudicating background investigations to make informed suitability and clearance eligibility decisions, ensuring compliance with federal government guidelines and security protocols.
* Mastered Department of Defense (DoD) and Intelligence Community (IC) personnel security regulations, maintaining a strong understanding of clearance processing procedures within both organizations.
* Applied expert technical knowledge to solve complex security-related issues, consistently leveraging laws, regulations, policies, and procedures to enhance the personnel security program.
* Adapted quickly to changing demands, demonstrating flexibility by prioritizing critical tasks to meet deadlines and ensure timely processing of government applicants.

**EDUCATION**

**Doctor of Management, concentration Information Systems and Technology |** Expected 2028

University of Phoenix, Goodyear, AZ

**Master of Business Administration** |

University of Maryland Global Campus, Adelphi, MD

**Master of Science in Cybersecurity |**

University of Maryland Global Campus, Adelphi, MD

**Master of Public Administration, Concentration: Emergency Management Homeland Security** |

George Mason University, Fairfax, VA

**Bachelor of Arts in Government and International Politics / Religious Studies (Double Major)** |

George Mason University, Fairfax, VA

*Magna cum laude graduate*

**TRAINING AND CERTIFICATIONS**

**Training:** Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Security Auditor (CISA), Security Specialist, Reid Technique of Interviewing & Interrogation, Continuity of Operations (COOP) Awareness, Physical Security Training, Derivative Classifier Training, SECURITY+, NETWORK+, ASIS Professional Security Professional (PSP), ASIS Certified Protection Professional (CPP), Internal Audit Subject Matter Specialist & Business Continuity Planning

**Certifications:**

* Artificial Intelligence for Business (Wharton)
* Certified Business Continuity Professional (DRI International)
* Executive Protection Certification