

Christopher Butler

Cybersecurity Governance, Risk & Security Assessment | Team Leadership & Executive Reporting

chris@chrisbcyber.com | linkedin.com/in/seabutler | chrisbcyber.com

PROFESSIONAL SUMMARY

Cybersecurity assessment, GRC, and vulnerability-management leader with 12 years across healthcare, government, higher education, and regulated-data environments. Former Business Information Security Officer who governed cybersecurity risk across roughly 150 applications, directed security assessments and remediation, and reported risk posture through senior director, VP, CISO/CIO, client, and board-level channels. Directly supervised cybersecurity staff, authored remediation and exception-governance standards, and applied frameworks such as HIPAA, CIS Controls, and NIST to practical risk decisions.

CORE COMPETENCIES

Capabilities: Security Assessment & Risk Analysis | Vulnerability Management | GRC & Exception Governance | Third-Party Risk | Application Security | Data Security | Security Policy & Standards | Executive & Board Reporting | Team Leadership & Staff Development

Framework Exposure: HIPAA | CIS Controls | NIST 800-53 | NIST CSF | PCI DSS | CMMC | NIST 800-171 | CJIS | FERPA | ISO 27001 | GLBA

Platforms & Tools: Archer | Onspring | Brinqa | ServiceNow Vulnerability Response | Tenable | WhiteHat | Checkmarx | Jira | Confluence | AWS | Azure

PROFESSIONAL EXPERIENCE

IT Project Manager – Security, Privacy & Data Governance

Aug 2025 – Aug 2026

University of Connecticut · Statewide Data Modernization

Storrs, CT

- Coordinated the security, privacy, and data-governance requirements of a statewide data-modernization program supporting 111 law enforcement agencies and 5 RMS vendors, aligning legal, compliance, privacy, and vendor stakeholders and driving 100% alignment with federal crash-data guidelines across 153 data elements.
- Assessed a proposed sensitive-data integration before build, identifying privacy and security gaps and translating RBAC, audit logging, anonymization, and secure-transmission needs into implementation requirements.
- Reviewed NIST 800-171 and CJIS implications for law enforcement data being ingested, tracking data-integration risk against applicable requirements.
- Owned a 34-item risk register (16 security, privacy, and third-party risks), keeping active risks visible through biweekly leadership escalation.
- Coordinated vulnerability discussions between the Engineering department and UConn's central Information Security Office.

Business Information Security Officer (BISO)

Feb 2023 – May 2025

The Cigna Group

Bloomfield, CT

- Owned cybersecurity GRC and risk-assessment governance for roughly 150 applications, including 30 business-critical systems handling PHI, PII, or PCI DSS data, leading recurring application-security and cyber-risk assessments across the portfolio.
- Authored remediation and exception-governance standards, defining exception criteria, approval thresholds, ownership, expiration dates, and compensating-control expectations with GRC partners.
- Raised and sustained vulnerability-management SLA compliance from 65% to 99% through recurring remediation reviews, exception governance, and leadership escalation.
- Directed cybersecurity analysts and shared security resources through application assessments, vulnerability scans, penetration tests, and risk reviews, translating outputs into remediation plans and leadership decisions.
- Reduced a third-party health-benefits administrator's aged high and medium-severity findings from roughly 30 to fewer than 10 through assessment review, remediation tracking, and control-evidence collection.
- Produced application-risk, vulnerability, exception, and remediation reporting for senior director, VP, CISO/CIO, client, and board-level channels.

Digital Operations Manager

The Cigna Group

May 2022 – Feb 2023

Bloomfield, CT

- Managed and developed a 6-person technical operations team, including two cybersecurity project managers, owning prioritization, workload management, performance feedback, and delivery standards.
- Trained application, business, and cybersecurity staff on release governance, security-remediation processes, tooling, and escalation paths.
- Standardized runbooks, checklists, dependency tracking, and go/no-go reviews, reducing release windows from 4 to 6 hours down to 2 to 3, and cutting rollbacks from roughly one in three releases to about one per quarter.

Cybersecurity Project Manager

The Cigna Group

Nov 2017 – May 2022

South Windsor, CT

- Directly managed a cybersecurity project manager for one year, owning goal-setting, performance reviews, and professional development across vulnerability-remediation and security-finding workflows.
- Coordinated application-security assessments and remediation across penetration testing, WhiteHat DAST, Checkmarx SAST, and GRC findings, driving remediation plans, retests, evidence collection, exception review, control validation, and Information Security sign-off.
- Eliminated a multi-year backlog of roughly 40 high and critical-severity vulnerabilities across 15 applications within three months, including 4 business-critical systems handling PHI, PII, or PCI DSS data.
- Led CIO-sponsored TLS 1.0 retirement across 100+ applications and coordinated urgent remediation for Log4j, legacy Apache Struts, and F5 web-security exposures across application, architecture, Information Security, change management, and release teams.

Technology Early Career Development Program

The Cigna Group

Jul 2014 – Nov 2017

Glasgow, UK & Bloomfield, CT

- Administered global PPM/agile tooling, including intake workflows, user access, configuration, reporting, training, and documentation for international technology teams.
- Completed rotational technology development program across software, infrastructure, portfolio governance, and global delivery teams, progressing into cybersecurity project delivery.

ASSESSMENT METHODOLOGY & GOVERNANCE

- Built practical security-assessment criteria spanning asset ownership, business function, data type, third-party dependency, vulnerability posture, MFA readiness, exception status, remediation evidence, and leadership approval path.
- Participated in enterprise CMMC assessment workshops and contributed to annual NIST CSF self-evaluations, translating results into remediation priorities and executive-ready reporting.

CERTIFICATIONS

CISSP – Certified Information Systems Security Professional, ISC2

2024

CCSK – Certificate of Cloud Security Knowledge, Cloud Security Alliance

2024

EDUCATION

M.S., Computer Science – Georgia Institute of Technology

2023

B.S., Computer Science – University of Glasgow

2014