

DAVINDERNAIN SINGH SEHGAL

Cybersecurity Leadership & Governance | Threat Detection & Response | Security Risk Assessment

Boston, USA – Relocating to Thane, Maharashtra, India | +91 9653282499 | Davindernain.sehgal@icloud.com
[linkedin.com/in/Davindernain](https://www.linkedin.com/in/Davindernain)

PROFESSIONAL SUMMARY

Cybersecurity professional with U.S. experience and an MS in Cybersecurity (Northeastern University) and hands-on ownership of information security for the City of Boston's Boston Public Library (BPL), covering 25+ locations and a multi-institution network and reporting directly to the CTO. Track record in incident response, identity security (100% MFA and password less rollout), third-party risk, vulnerability management, and governance aligned to NIST, CISA, and ISO 27001, working alongside the City of Boston's central Cybersecurity Operations team. Secured a \$250,000 (~₹2.4 Cr) security grant, cut malicious bot traffic by 70%, and raised phishing detection and reporting by 90%. Experience across municipal government, non-profit, startup, and consulting environments in the USA and India.

EDUCATION

Northeastern University, Boston, MA, USA

May 2023

Master of Science in Cybersecurity

Relevant Coursework: Software Vulnerabilities & Security, Security Risk Assessment and Audits, Network Security Practices, Security Governance Risk & Compliance (Cyberlaw), Digital Forensics, Decision Making in Critical Infrastructure.

University of Mumbai, Mumbai, India

Jun 2021

Bachelor of Science in Computer Science

Relevant Coursework: Data Structures, Cloud Computing, Ethical Hacking, Information Retrieval.

TECHNICAL SKILLS

Expertise: Threat Detection, Risk Assessments & Audits, Policy Creation & Implementation, Vulnerability Management, Security Awareness Training & Phishing Simulation, Penetration Testing, Digital Forensics, OSINT/Reconnaissance

SIEM Tools: Microsoft Defender, Sentinel One, Splunk, QRadar

Security Tools: Nmap, Wireshark, Metasploit, Burp Suite, Nikto, Bitdefender, IBM X-Force, Kali Linux tools, Web Application Firewalls (WAF), pfSense, Snort IDS, FTK Imager, Autopsy, Spiderfoot, Maltego, Shodan

Cloud: Amazon Web Services (AWS), Microsoft Entra ID (Azure Active Directory)

Frameworks & Compliance: ISO 17799/27001, GDPR, HIPAA, HITRUST, CISA, NIST (800-30/800-53), OWASP, COBIT, PCI DSS, NICE, SOC 1, SOX, MITRE ATT&CK

Languages: SQL, Python, Java, Bash Scripting

EXPERIENCE

City of Boston, Boston, MA, USA

Nov 2023 – Present

Boston Public Library (BPL) | IT Cybersecurity Analyst & BPL Cybersecurity Officer

Sole cybersecurity resource for the City of Boston's Boston Public Library system: the Central Library, all 25 branch locations, and the Metro Boston Library Network (MBLN), a shared network and staffing consortium linking additional public, school, and college libraries across the region. Acts as the bridge between the City of Boston's central Cybersecurity Operations team and BPL leadership, owning security strategy end-to-end with no dedicated security team beneath or above this role at the library level.

- Held Cybersecurity Officer responsibilities for the library system, reporting directly to the CTO as the single point of accountability for security strategy, incident response, governance, auditing, risk, and cybersecurity metrics reporting across 25+ locations and the Metropolitan Boston Library Network (MBLN), a multi-institution network.
- Secured a \$250,000 (~₹2.4 Cr) FCC Cybersecurity Pilot Program grant by leading research, documentation, and the application with multiple departments, funding network security infrastructure upgrades.
- Directed incident response for a high monthly volume of security incidents, triaging alerts daily and leading investigation, containment, and remediation across Network, Server, Application, Help Desk, and A/V teams; liaised with law enforcement and City of Boston counterparts on significant incidents.
- Built scenario-specific incident response strategies and playbooks defining the response for each type of incident, along with playbooks for security operations, access management, and endpoint security, standardizing procedures and improving organizational readiness.
- Led organization-wide rollout of MFA and password less authentication (Microsoft Authenticator, passkeys), achieving 100% organizational MFA coverage through user guides, training, and enforced controls.
- Established the security evaluation framework for new vendors, products, and acquisitions, and led third-party risk assessments with multiple departments against NIST and CISA guidance, assessing controls, compliance, data protection, cost, and business value before purchase or implementation.

- Led a multi-year initiative to decommission and upgrade end-of-life (EOL) servers and software, bringing 100+ systems to current security standards and materially reducing the attack surface.
- Deployed and tuned a Web Application Firewall (WAF) protecting public-facing infrastructure, reducing malicious bot traffic and automated attack attempts by 70%.
- Ran the staff security awareness program with recurring phishing simulations that increased phishing detection and reporting rates by 90% over 8 months; developed training on authentication, phishing, and account protection.
- Designed and taught public cybersecurity literacy sessions with community learning programs for patrons of all ages across BPL branches.
- Led internal vulnerability assessments and penetration testing (Metasploit, Nmap, Burp Suite), identifying critical vulnerabilities in public and staff-facing systems and driving remediation through targeted best-practice fixes.
- Documented information security standards and policies aligned with NIST and CISA, guiding procurement, design, maintenance, and retirement decisions across the technology lifecycle; analyzed processes for security risk with the Technology Process Improvement Owner and recommended procedural changes.
- Managed core security systems (IDS/IPS, anti-malware, firewalls, encryption) and enterprise asset and license inventories with the Help Desk Manager; designed separate risk-based configurations for public-access versus staff computers across dozens of locations.
- Directed business continuity and disaster recovery planning with the Server and Network teams, documenting, maintaining, and testing recovery procedures.
- Worked with Server, Network, and Web Services teams to build security into system installation, configuration, and maintenance, and acted as point of contact for external vendors on issues beyond internal scope.
- Coordinated with the City of Boston Cybersecurity Operations team to research, select, and document security best practices, representing BPL in city-level security governance.
- Advised IT leadership on emerging threats, vulnerabilities, and countermeasures, shaping technology decisions before production; tracked the threat landscape through security professional organizations, listservs, forums, and threat intelligence.

Village Book Builders (Non-Profit), Boston, MA, USA

Apr 2023 – Nov 2023

Cybersecurity Associate (Volunteer)

- Spearheaded the development and implementation of security policies using the ISO 27001/27002 compliance framework.
- Conducted in-depth risk assessments with cross-functional teams, identifying potential threats and proposing mitigation strategies that reduced projected impact costs by over \$130,000 (~₹1.25 Cr).
- Led the development and optimization of custom-tailored incident response plans for ransomware attacks and emerging security threats, minimizing potential damage.
- Customized Standard Operating Procedures (SOPs) for seamless adherence to compliance standards throughout the organization.
- Organized company-wide IT risk training sessions, including presentations and quizzes, fostering a security-conscious culture for full-time and part-time employees.

Commonwealth Financial Network, Waltham, MA, USA

Jan 2023 – Apr 2023

Information Security Capstone

- Built a streamlined operational risk registration and monitoring system using Trello and Jira, improving coordination across 7+ departments.
- Used Agile methodology to meet team sprint deadlines every 3 weeks, ensuring timely completion of project deliverables.
- Authored and presented educational materials and technical documentation for stakeholder training and adoption.
- Used Power BI, Excel, and Microsoft Forms to register and present operational risks statistically, reducing overall operational risk.

YourDigitalBro Pvt Ltd, Mumbai, India

Sep 2020 – Jun 2021

IT Security Intern

- Implemented basic security tooling to monitor and analyze security events, increasing proactive incident detection and response capability by 35%.
- Deployed firewalls and IDS/IPS for increased visibility and security, reducing unauthorized access attempts by 50%.
- Administered infosec policies safeguarding PII for 550+ clients monthly.
- Delivered security awareness training for employees, reducing phishing incidents and malware infections by 25%.

Freelance, Mumbai, India

Aug 2018 – May 2021

IT Consultant

- Assessed client technical needs and recommended appropriate hardware and software.
- Helped 87 clients implement strong security controls, including anti-virus, anti-malware, and data encryption.
- Achieved a 95% success rate resolving hardware/software issues within 24 hours, minimizing downtime.

- Educated 50+ clients on strong passwords, two-factor authentication, and security best practices; trained non-technical individuals to recognize phishing and malware.

PROJECTS

Security Risk Management and Assessment | Northeastern University, Boston, MA **2022**

- Curated threat-vulnerability pairs to assess attack likelihood and document potential impact on assets valued at over \$600,000.
- Conducted qualitative and quantitative risk assessments using the HGA case study and NIST Framework.

Incident Response Playbook | Northeastern University, Boston, MA **2021**

- Devised IR team guidelines covering all NIST incident-response framework phases for handling security breaches (unauthorized access, SQL injection, and data leaks).
- Mapped over 92% of MITRE ATT&CK techniques, reducing response time by 15 days per stage.

Passive Reconnaissance | Northeastern University, Boston, MA **2022**

- Conducted OSINT-based security assessments of two e-commerce platforms using 8+ tools, including Spiderfoot, Maltego, Shodan, and Dig, identifying exposed ports, DNS records, and CVEs.
- Delivered technical reports with actionable remediation recommendations to strengthen each platform's security posture.

Digital Forensics of Windows Desktops & Mobile Devices | Northeastern University, Boston, MA **2022**

- Investigated insider-threat, employee-harassment, and malware-infection scenarios across four systems and external devices using FTK Imager and Autopsy.
- Maintained strict chain-of-custody protocols throughout evidence extraction and preservation to ensure legal admissibility.

GRC Response to Ransomware | Northeastern University, Boston, MA **2022**

- Authored a governance-risk-compliance (GRC) research paper analyzing ransomware attack mechanisms and developing tailored response strategies.
- Consolidated 5+ ransomware prevention and incident-response methodologies into actionable GRC best practices.

IDS/IPS Implementation | Northeastern University, Boston, MA **2023**

- Deployed pfSense firewall and Snort IDS with zero-trust, default-deny policies across two local networks.
- Used Nmap scanning and real-time packet inspection to identify and close vulnerabilities, improving the security posture of both networks.

Digital Forensics (Research Paper) | Northeastern University, Boston, MA **2022**

- Produced an in-depth research paper and strategic guide spanning three branches of digital forensics.
- Improved new investigators' case-handling effectiveness by 20% following adoption of the guide.

PROFESSIONAL DEVELOPMENT

- Actively preparing for CISSP (Certified Information Systems Security Professional); completed self-study across all 8 CISSP domains.

MEMBERSHIPS & ASSOCIATIONS

- Member of (ISC)², CISA, and SANS.
- Member of MS-ISAC and TLDR Cybersecurity to stay current on infosec trends.

EXTRACURRICULAR

- AIG Shields Up: Virtual Experience Program, Incident Response Team Leader: addressed zero-day vulnerabilities and coordinated a team to assess, contain, and mitigate threats.
- Mastercard: Cybersecurity Virtual Experience Program, Phishing Campaign Analysis: simulated and evaluated a sophisticated phishing campaign.
- TryHackMe Jr. SOC Analyst (SOC Level 1), Triage Specialist: monitored and investigated alerts, devised IDS signatures, and managed security tools.

PERSONAL DETAILS & INTERESTS

Languages Known: English, Hindi, Marathi, Punjabi

Notice Period / Availability: 30 – 45 days (Negotiable)

Location Preference: Mumbai, Maharashtra

Interests: Music (ukulele, music production), learning about emerging technology, competitive and RPG gaming, travel, movie/TV and anime.