



Mobile No: +91-9880083147

Email: amitprakash22nov@gmail.com

AMIT PRAKASH

linked-in: www.linkedin.com/in/ap-itsecurity

Seasoned Cybersecurity Executive with over 19 years of success leading enterprise security programs across banking, financial services, and healthcare. CISSP, CISM, and CEH certified, with deep expertise in regulatory and compliance frameworks including PCI-DSS, SOX, FFIEC, NYDFS, HIPAA, MeitY, SEBI, DSCI, HITRUST, NIST CSF, NIST 800-53 etc. Proven ability to reduce cyber risk, drive security modernization, and lead large-scale incident response across complex, highly regulated environments. Recognized for building and mentoring high-performing security teams, leading enterprise GRC and cloud security initiatives, and aligning cybersecurity strategy with organizational goals. Trusted advisor to executive, clinical, and business leadership committed to fostering security first cultures while enabling innovation and digital transformation.

PROFESSIONAL SYNOPSIS

Leadership and Strategy: Proven ability to develop and execute cybersecurity strategies that align with business goals. Experienced in partnering with executive leadership and board members to embed security into operational processes, ensuring the protection of critical assets from evolving digital threats.

Risk Management and Compliance: Skilled in identifying, assessing, and prioritizing cybersecurity risks. Implements proactive risk mitigation strategies, leads incident response efforts, and ensures ongoing compliance with regulatory frameworks and industry standards such as ISO/IEC 27001, CIS, COBIT, PCI DSS, RBI, DPD, GDPR, FedRAMP, SOC2, NIST etc.

Technical Expertise: Extensive knowledge of cybersecurity technologies and solutions, including firewalls, intrusion detection and prevention systems (IDS/IPS), identity and access management (IAM), encryption, endpoint protection (EDR, DLP), and security information management (SIEM) tools.

Cloud Security: Deep expertise in designing and securing cloud environments across AWS, Azure, and GCP. Skilled in conducting comprehensive risk assessments to identify vulnerabilities, prioritize risks, and implement mitigation strategies in both cloud and on-premises data center environments. My approach ensures robust security, regulatory compliance, and seamless integration with enterprise systems. I proactively manage emerging threats to safeguard hybrid infrastructures and maintain business continuity.

Strategic Alignment: A key strength is aligning cybersecurity initiatives with organizational goals, regulatory requirements, and business objectives to drive resilience, operational efficiency, and long-term success.

Achievements

Spearheaded a bank-wide cybersecurity transformation at **ICICI Bank**, achieving **100% compliance** with **ISO 27001**, **RBI** regulations, and the **Digital Personal Data Protection (DPDP) Act**, through rigorous governance, policy enforcement, and security architecture redesign.

Architected and implemented secure hybrid cloud infrastructures across **AWS, Azure, and GCP** for **50+ mission-critical applications**, enabling scalable, compliant, and resilient platforms for banking operations, with security controls embedded across IaaS, PaaS, and SaaS layers.

Led 25+ comprehensive risk assessments and security audits, identifying high-risk vulnerabilities across on-prem and cloud environments. Directed and tracked remediation strategies that significantly reduced the threat landscape.

Directed large-scale security programs that safeguarded **10,000+ endpoints, 50+ firewalls**, and **multi-region data centers**, ensuring consistent protection across internal systems and customer-facing services.

Maintained a **zero major breach record** during tenure across **three organizations**, underscoring a proactive and risk-informed security leadership approach.

Built and led a high-performing cybersecurity team of 20+ professionals, spanning architecture, GRC, SOC operations, and incident response. Drove alignment between security strategy and business objectives, fostering a resilient and agile security culture.

Integrated advanced security technologies, including **SASE, SD-WAN, IAM, PAM, DLP, and SIEM** solutions, ensuring seamless interoperability across a **multi-vendor ecosystem** while enhancing visibility, access control, and threat detection capabilities.

Achieved **15% cost optimization** in cybersecurity operations through **vendor consolidation, automation, and strategic cloud migration**, demonstrating a balance of operational efficiency and strong risk management.

Progressive Career Growth in 19+ years.

1. **Advance Security Consulting Lead** Bayer AG – Global IT, Cybersecurity Division Jan 2025 to till date
2. **Cloud Security Head**,(Information Security Group) ICICI Bank, Dec 2023 to Dec 2024
3. **Sr. Technical Consultant**, (Network Security Engineering) DXC Technology (erstwhile part of Hewlett Packard Enterprise, Bengaluru, India.). Sep 2015– Dec 2023
4. **Sr. Technical Lead**, (Security) Happiest Minds , Bengaluru, India. Oct 2014 to Sep 2015
5. **Technical Lead**,(ESRM) Cognizant Technology Solutions Bengaluru, Feb 2014 – Oct- 2014.
6. **Senior Engineer, Security Management**, Wipro Technology, Bengaluru, India, Feb 2010- Jan 2014.
7. **Security Analyst**, Next Edge Software Solutions Pvt Ltd., Bengaluru, India, Dec 2008 – Jan 2010.
8. **Escalation Engineer (Symantec AV Support)**, E4E Business Solutions India Ltd., Bengaluru, India, April 2007 – Dec 2008.

Competencies

Cybersecurity Leadership & Governance: Cybersecurity Strategy & Executive Leadership; Enterprise Security Governance & Risk Management (GRC); Regulatory Compliance: NIST, ISO 27001, HIPAA, PCI-DSS, GDPR; Board-Level Communication & Reporting; Cybersecurity Policy Development & Enforcement; Security Awareness & Training Programs; Team Building & Cross-functional Leadership. **Identity & Access Management (IAM):-** Privileged Access Management (PAM); Identity Lifecycle Management (IAM); Single Sign-On (SSO), Multi-Factor Authentication (MFA); Federation & Role-Based Access Control (RBAC); Active Directory, Azure AD, Okta, CyberArk. **Threat & Vulnerability Management:-** Threat Intelligence & Dark Web Surveillance; Security Incident Management & Breach Response; Vulnerability Management & Penetration Testing (VAPT); Security Operations Center (SOC) Oversight; Endpoint Detection & Response (EDR); SIEM & SOAR Platforms (e.g., Splunk, McAfee Nitro); Red/Blue/Purple Team Exercises. **Network & Infrastructure Security:-** Firewall, IDS/IPS, WAF, Proxy, Load Balancers; DNS Security, SASE, SD-WAN; Network Design, Sizing, and Architecture Planning; Routing Protocols: OSPF, EIGRP, BGP, RIP, IGRP; Protocols: OSI, TCP/IP Suite (DNS, DHCP, HTTP/S, SMTP, etc.); Tools: Wireshark, SolarWinds, PRTG, Nessus. **Cloud & Data Center Security:-** Cloud Security (AWS, Azure, GCP, Hybrid Cloud Architectures); Cloud Governance, Workload Protection, CSPM, CWPP; Data Center Security & Segmentation (Cisco DNA Center, ACI); Public, Private & Multi-Cloud Security Controls; DNS-layer Security, Cloud-native Firewalls; Encryption Technologies: TLS, AES, PKI, KMS. **Data Protection & Privacy:-** Data Classification & Loss Prevention (DLP); CASBs for Cloud Application Security; Secure Backup & Business Continuity Planning; Data Governance & Retention Policies; Data Masking, Tokenization, Anonymization. **Secure Architecture & Engineering:-** Zero Trust Architecture & Microsegmentation; DevSecOps Integration into CI/CD Pipelines; Secure SDLC, Threat Modeling, Code Scanning; Architecture Reviews for Application and Infrastructure Security; Automation via Python, PowerShell for Security Tasks; Design Tools: Microsoft Visio, Lucidchart. **Enterprise IT & Collaboration Solutions:-** Enterprise Networking: Cisco, Meraki, Aruba, Extreme; Wireless Networking (WiFi 6): Cisco, Ruckus, Aruba; Unified Communications: Cisco CME, CUCM, Jabber, WebEx, Microsoft Teams; Network Capacity Planning & Sizing.

Certifications

1:Fortinet NSE4,2:Microsoft Azure Fundamental,3:Cisco Certified Network Associate,4:CEH v7,5:CCIE Security (Written),6:AWS Certified Solutions Architect,7:Checkpoint CCSA,8:CCSE, 9:CISM,10:CISSP, 11:CRISC, 12: PMP 13: Professional Agile Leadership 1 (PAL)

Educational Qualification & Personal Detail

Qualification:

M.Tech: (Data Science & Machine Learning) PES University 2021- 2023

B.E. :(Information Science) V.T.U pursuing Ph.D.

Date of Birth: 22nd Nov 1979.

Languages Known: English,Hindi.

Nationality: Indian.

Marital Status: Married.

Location: Bengaluru.

Bayer AG – Global IT, Cybersecurity Division
Advance Security Consulting Lead Jan 2025 to till date

Strategic cybersecurity executive and direct report to the Global CISO, accountable for driving security transformation, governance, and enterprise resilience across Bayer's digital, cloud, and regulated IT environments. Lead cross-functional programs aligned with Bayer's global cybersecurity strategy, supporting operations in life sciences, pharmaceuticals, and crop science.

Serve as a primary advisor to the CISO on matters of architecture, risk management, compliance posture, and technology modernization. Translate executive vision into actionable programs while managing stakeholder engagement, audit preparedness, and operational delivery.

Key Skills:

Trusted CISO Advisor | Global Cybersecurity Execution | Cloud Security Architecture (AWS, Azure, GCP) | Enterprise Risk Management | Regulatory Compliance (ISO 27001, GDPR, RBI, DPDP) | Cybersecurity Governance | Audit Leadership | Incident Response | SIEM/PAM/DLP Integration | Executive Reporting | High-Performing Team Leadership | Stakeholder Influence

ICICI Bank Ltd.

Chief manager II (Information Security Group) Dec 2023 to Dec 2024

Cybersecurity Leadership – Governance, Risk & Compliance (GRC)

Served as a senior cybersecurity leader reporting to both the CISO and CRO, driving enterprise-wide governance, risk, and compliance (GRC) strategies. Actively participated in executive steering committee meetings, influencing decision-making on cyber risk, regulatory priorities, and strategic technology initiatives. Operated as a key conduit between cybersecurity operations, executive leadership, regulators, and cross-functional stakeholders.

Leadership Impact & Responsibilities:

Enterprise GRC Strategy: Directed the end-to-end design and execution of cybersecurity programs, policies, and control frameworks to align with strategic business objectives and executive risk appetite.

Regulatory Engagement & Compliance: Managed all regulatory interfaces, including SEBI, RBI, and ISO 27001. Led successful audit cycles, regulatory submissions, and certification renewals with no major findings.

Risk Management & Assessment: Conducted independent risk assessments and deep-dive analysis, facilitating risk prioritization and mitigation with full traceability and executive reporting through dashboards.

Executive Reporting & Board Communication: Provided GRC briefings and risk intelligence to the CISO, CRO, and Board-level steering committees, shaping cybersecurity roadmap and policy governance.

Policy & Control Effectiveness: Evaluated and enhanced security controls across systems and processes; implemented continuous monitoring and improvement cycles aligned with ISO and NIST frameworks.

Awareness & Culture Building: Launched and championed cybersecurity awareness initiatives across all business units, cultivating a culture of accountability and proactive security behavior.

Third-Party Risk Oversight: Led due diligence and risk reviews of third-party vendors and partners, ensuring adherence to contractual and regulatory obligations while mitigating external threat exposure.

Operational Excellence: Ensured timely execution of core security practices such as log reviews, vulnerability assessments (VAPT), and secure SDLC activities across all environments.

Key Skills:

Cybersecurity Governance | Executive Risk Reporting | Regulatory Compliance (SEBI, RBI, ISO 27001) | Board-Level Engagement | Risk Assessment & Prioritization | GRC Leadership | Security Awareness & Culture | Third-Party Risk Management | Strategic Policy Development | Audit & Certification Management | Cyber Risk Dashboarding | Vulnerability & Threat Management

DXC Technology (erstwhile part of Hewlett Packard Enterprise, Bengaluru, India.)

Sr. Technical Consultant (Network Security) Sep 2015– Dec 2023

Cybersecurity / Network Security Architect – Enterprise Services Global Engineering & Technical Consulting

Architected and delivered secure network and cloud solutions across complex enterprise environments, including Data Centers and multi-cloud infrastructures (AWS, Azure, GCP, Aviatrix). Spearheaded the design of scalable, compliant security architectures encompassing network segmentation, identity and access management, endpoint protection, and encryption. Applied deep expertise in security frameworks (ISO, GDPR, NIST, COBIT) to perform risk assessments, guide regulatory compliance, and support secure digital transformation initiatives.

Led end-to-end architectural planning for cloud and network security, integrating security-by-design principles into DevOps pipelines using Ansible, Terraform, and Python. Conducted comprehensive assessments of threats and vulnerabilities, implementing layered defenses and automated remediation strategies. Directed enterprise-wide cybersecurity programs, incident response efforts, and the deployment of advanced controls to secure critical assets.

Collaborated with cross-functional teams to align security architecture with business and IT strategies, ensuring seamless integration into SDLC and cloud migration efforts. Evaluated emerging technologies and third-party solutions, strengthening the organization's security posture and vendor compliance landscape.

Key Achievements:

Led the architecture and implementation of secure hybrid network infrastructures, overseeing legacy-to-cloud migration initiatives.

Defined cloud security strategies and enforced governance across AWS, Azure, and GCP platforms.

Managed risk identification, mitigation planning, and closure tracking across enterprise environments.

Delivered technical leadership and mentorship to a high-performing security team, driving alignment with enterprise objectives.

Orchestrated penetration tests, audits, and security reviews to validate architectural resilience and regulatory compliance.

Key Skills:

Network & Cloud Security Architecture | Cybersecurity Strategy | Risk & Compliance (ISO, GDPR, NIST, COBIT) | Public Cloud Security (AWS, Azure, GCP, Aviatrix) | Infrastructure-as-Code (Ansible, Terraform, Python) | DevSecOps Integration | Identity & Access Management (IAM) | Incident Response & Threat Mitigation | Security Governance | Secure SDLC | Third-Party Risk Management

Happiest Minds, Bengaluru, India.

Sr. Technical Lead (IT Security) Oct 2014 – Sep 2015

Cybersecurity Specialist – Solution Architecture & Pre-Sales (Cloud & Data Security)

Delivered end-to-end **cloud and data security solutions**, focusing on **Azure, AWS**, and hybrid environments. Designed **security blueprints**, selected technologies, and led the setup of **SIEM and SOC operations** for mission-critical use cases. Played a key role in **pre-sales strategy**, preparing **RFPs, white papers, and technical demos** to support client acquisition and retention. Conducted assessments of client environments, identified security gaps, and crafted tailored solutions covering **IaaS, PaaS, and SaaS**. Partnered with cross-functional teams to align customer requirements with solution design and contributed to product innovation through field feedback.

Key Skills:

Cloud Security (Azure, AWS) | SIEM Implementation | SOC Design | Pre-Sales & Solution Consulting | RFP/RFI/RFQ Support | Network & Data Security | Firewall & DLP | Technical Demonstrations | Security Framework Design | Client Engagement | Proof-of-Concept (PoC)

Cognizant Technology Solutions, Bengaluru, India. Client :- Banking

Technical Lead (ESRM) Feb 2014 – Oct 2014

Technical Lead – Infrastructure & Threat Response

Designed and implemented robust network security architectures, including **firewalls, IDS/IPS, VPNs**, and remote access solutions. Conducted **vulnerability assessments and penetration testing** to identify and mitigate risks. Collaborated with cross-functional teams to embed security in new systems and applications. Led **incident detection and response**, monitored network traffic, and executed remediation efforts. Authored and maintained security policies, procedures, and documentation to ensure compliance and operational readiness.

Key Skills:

Firewall Design | IDS/IPS | VPN | Vulnerability Assessment | Penetration Testing | Security Incident Response | Policy Development | Network Traffic Analysis

Wipro Technology, Bengaluru, India. Client :- more than 30 clients (Banking, Retailers, Telecom etc.)

Senior Engineer (Security Management) Feb 2010-Jan 2014

Security Consultant – Enterprise Security Solutions, Wipro

Aug 2011 – Sept 2013 (Client: MTN Telecom – Uganda)
Feb 2010 – Aug 2011 (SOC Operations – GSRTC, Mysore)

Led a cross-functional security team delivering enterprise-grade solutions for high-stakes clients in the **telecom and BFSI** sectors. Specializing in **compliance-driven environments**, provided end-to-end security strategy, architecture, and operations management aligned with **ISO/IEC 27001** and risk frameworks relevant to regulated industries. Conducted **infrastructure assessments, vulnerability and penetration testing**, and led **data center migrations**, ensuring robust security controls and zero disruption. In healthcare contexts (internal proof-of-concept and client consulting), prioritized **data privacy, endpoint protection**, and **HIPAA-aligned** control implementation strategies.

Key Achievements:

Delivered **secure data center migration** and policy governance programs for MTN Telecom, ensuring uninterrupted service and regulatory compliance. Oversaw **multi-vendor security architecture** design and implementation (firewalls, IPS/IDS, DLP, proxy, AV) to meet strict regulatory demands of telecom and BFSI clients. Conducted **capacity planning and risk assessments** for secure scaling of critical systems in alignment with business continuity goals. Executed **ISO/IEC 27001-based audits** and remediation planning to support BFSI client readiness for RBI and SOC 2 compliance reviews. Upgraded critical infrastructure using **L3/L4-level firewall and endpoint security patching**, aligned with emerging threats in healthcare and telecom networks.

Key Skills:

Azure | AWS | Network Security | Firewall Management (Check Point, Cisco, Fortinet, Juniper) | IPS/IDS | Proxy & DLP | Antivirus (Symantec, McAfee, Trend Micro) | VA/PT | ISO/IEC 27001 Compliance | Data Center Migration | Capacity Planning | Security Architecture | Performance Optimization | Risk Management

Next Edge Software Solutions Pvt. Ltd., Bengaluru, India. Client:- Mashreq bank U.A.E.

Security Analyst, Dec 2008 – Jan 2010.

Security Analyst – SOC, Mashreq Bank, Dubai

Led threat detection, incident response, and proactive threat hunting in a high-stakes banking environment. Monitored SIEM alerts, conducted vulnerability assessments, and designed secure network architectures using multi-vendor firewalls, IDS/IPS, VPNs, and proxies. Ensured regulatory compliance by documenting incidents, participating in security drills, and maintaining up-to-date policies and procedures. Collaborated with cross-functional teams to implement security controls across new applications and infrastructure.

Key Skills:

SOC Operations, SIEM, IDS/IPS, Network Security, Threat Hunting, Firewall Management, Incident Response, Vulnerability Assessment, Security Audits

E4E Business Solutions India Ltd., Bengaluru, India

Escalation Engineer (Symantec AV Support), April 2007 – Dec 2008.

Technical Support Engineer – Endpoint Security Operations

Provided technical support for Symantec Antivirus infrastructure, ensuring seamless operation and protection of enterprise endpoints. Responsibilities included analyzing security logs, investigating incidents generated by security tools, and troubleshooting antivirus-related issues in real time. Participated in cross-functional calls to resolve escalated support cases, contributing to enhanced endpoint resilience and user satisfaction.

Key Skills:

Symantec Endpoint Protection, Antivirus Management, Security Incident Analysis, Log Review, Technical Troubleshooting, Endpoint Security, Customer Support, Root Cause Analysis, ITIL Processes