Dhruv Pandya, CISM CISA CIPM CIAM

Address: Camarillo, CA • **Contact**: (805) 302-2822 • **Email**: dhruv.pnd@gmail.com /dhruvpandya.net

INFORMATION SECURITY PROFESSIONAL
Information & Content Security| Compliance| Systems Security

PROFESSIONAL PROFILE

Motivated and experienced senior Information Security professional with a master's in computer science and 7 years combined experience in working and designing organizational security programs. A business leader and articulate communicator adept at closing critical loopholes, maximizing security options, and staying ahead of current risks. Proven background in managing technical projects from inception to completion and translating complex requirements and expectations on the use of technology services into operational solutions. Possess strong understanding of cloud computing services and security systems architecture, partners with key business leaders and technical leads, and excels at providing expert consultation and relationship management.

ACHIEVEMENTS

- 40 under 40 upcoming leaders in Tri-County by Pacific Coast Business Times
- Managed Information security for J.D. Power and grew the organization's capacity for business.
- Served as a single senior security resource for 6 global offices and managed a team of 2 security resources.
- Facilitated the successful merging of J.D. Power Company and gained 6 acquisitions during Covid integrating and implementing security technologies.
- Spearheaded a million USD security budget and an organization of 2500 plus resources.
- Supervised and trained security professionals

EDUCATION

MS Computer Science	**Dec 2017**
California State University, Channel Islands	*Camarillo, CA*
B. Engineering Computer Engineering	**Jul 2014**
Savitribai Phule Pune University, Pune	*Maharashtra, India*

PROFESSIONAL EXPERIENCE

Director, Information Security	**Oct 2022 - Present**
Wistia	*Remote*

- Creating and Driving Information Security governance strategies for the organization
- Introduce Security Risk Management program
- Implement a vulnerability management program.
- Educate employees -- at all levels -- with helpful and relevant security and data privacy trainings.
- Vet vendors, sub processors and any other third parties who may handle sensitive data.
- Derive maximal benefit from white hat security researchers via bug bounties and other programs.
- Proactively monitor for and respond to urgent issues and CVEs that would otherwise put us at risk.
- Understand customers' security concerns and address them through action or explanation.

Senior Manager, Information Security	**Oct 2021 – Oct 2022**
J.D. Power	*Westlake Village, CA*

- Security Lead overseeing the organizational security after the CISO was let go in 2019.
- Responsible for information policy development and oversight, Security Governance, Risk and Compliance function.
- Partner with multiple business units effectively exhibiting the security assurance to clients and increasing revenue.
- Identify critical information assets and assess the risks associated with data management practices.
- Implemented and devised a strategy for implementing organizational DNS filter tool and restricting traffic from sanctioned countries.
- Develop, update, and implement the security incident response plan. Document all activities during an incident and provide leadership with status updates during the incident life cycle.
- Communicate with users, management, customers, and vendors with information security related matters / audits / regulatory requirements / policies, etc.
- Support IT system owners with Disaster Recovery and Business Continuity Planning and testing. Maintain DRP/BCP documentation for all major IT areas.

Dhruv Pandya, CISM CIAM

- Work closely with other teams such as the JD Power technology teams, as well as third party security service providers.

Information Security Specialist   Jul 2018 – Oct 2021
J.D. Power   *Westlake Village, CA*

- Successfully lead and managed the effort for achieving and maintaining SOC2 Compliance for the organization.
- Designed and implemented monitoring strategy for the different monitoring tools like Security Incident Event Management (SIEM), Email Gateway, Intrusion Detection System (IDS) /Intrusion Prevention System (IPS), Endpoint Security Forensics. (Alert Logic for AWS, Proofpoint Technologies for email security, Symantec Endpoint protection, Symantec IDS, IPS).
- Strengthened the email security by developing a domain-based Message Authentication Reporting and Conformance (DMARC).
- Oversaw vulnerability management for the enterprise and constantly researched threat landscape updating the defense capabilities by proposing in-house and/or off shelf solutions.
- Created and presented business case on various security subjects to the executive management and edited information security and data protection policies as per ISO 27001/27002 standards to ensure compliance.

Information Technology Volunteer   Jan 2018 – Jul 2018
Turning Point Foundation   *Ventura, CA*

- Aided the Non-profit Foundation with an in-house system security audit and developed Payroll application and a user database.
- Developed and implemented strategy for the Identity management of users, analyzed the vendor requests and quotations for the current services, and laid out a plan to upgrade the infrastructure to AWS.

IT Infrastructure Student Assistant   Oct 2015 – Aug 2017
Technology and Innovation, CSU Channel Islands   *Camarillo, CA*

- Installed Cisco, Alcatel Lucent switches, Aruba wireless access point. Enterprise printer and utilities, Cisco VoIP phones, Network Rackspace, Network UPS, Emergency Analog phones and over 3500 feet of onsite Cat 3, 5e and 6 LAN cables.
- Conducted successful weekly and biweekly maintenance of Campus Emergency Talk- a-Phone, Enterprise Printers, Server disk collection, Data center operations, network Rackspace, network UPS, connectivity across 100 telecom rooms.
- Managed inventory for the network equipment, documentation for printing manuals, Pharos printer administrator and user console, Nagios network and server log monitoring dashboard.
- Performed troubleshooting using standard ticketing systems, for wired network issues, enterprise wireless issues (BSGP).

R E S E A R C H   E X P E R I E N C E

MS. Candidate, Graduate Student Researcher   May 2016 – Dec 2017
CSU Channel Islands   *Camarillo, CA*

- Developed a Robust Software tool as requested by Southern California High Technology Task Force (Ventura County, LA County and Santa Barbara Law enforcement).
- Constructed a test-driven application using Amazon Web Services AWS and Scapy/Python.
- Implemented a 24 X 7 Packet parsing tool which extracts details ruled by program admin, from the incoming packets and upload them to a MySQL database hosted on server.
- Developed using, Scapy, Libpcap, Tcpdump, Python, HTML5, HTMLForms, PHP, MySQL, Bootstrap, SDLC.

T E C H N I C A L   S K I L L S

- **Compliance Frameworks:** SOC Type 1,2 and 3, TISAX, PCI, GDPR, CCPA, GLBA, HITRUST-9.4,9.3,9.2)
- **Information Security Framework:** ISO, NIST, SIG, CIS
- **Cloud Services:** Google cloud services, Amazon EC2.
- **Network & Security:** VPN, IDS/IPS, Palo Alto Panorama, SIEM-Alertlogic, Proofpoint TAP.
- **Endpoint Security:** Carbon Black Advanced XDR, Symantec SEP and EDR, Bitdefender, Endpoint Privilege Management, DLP

C E R T I F I C A T I O N S

Certified Information Security Manager: Information Systems Audit and Control Association (ISACA), Credential:221850130

Certified Information Security and Systems Professional: Infosec Train, Credential ID ISTT227323

Certified Identity and Access Manager: Identity Management Institute

Proofpoint Accredited Administrator - Targeted Attack Protection (TAP)- Proofpoint University

Proofpoint Accredited Administrator - Email Protection Gateway -Proofpoint University

CORE COMPETENCIES

Design and Strategy **|** Troubleshooting **|** Updating & Installation Maintenance **|** Training & Awareness **|** Merger and Acquisition (M&A) Security **|** Incident Response **|** Compliance Oversight **|** Policy Development & Enforcement **|** Incident & Report Management **|** Stakeholder Engagement **|** Risk Assessments **|** Best Practices **|** Flexibility **|** Process Improvements **|** Leadership & Supervision **|** Configuration Management **|** Network Security **|** Database Management **|** Application Coding **|** Project / Program Management **|** People Management **|** Security Technology **|** Cloud Security (AWS &GCP) **|** Vulnerability Management **|** Data Loss Prevention (DLP) **|** Security Incident & Event Management (SIEM) **|** Identity & Access Management (IAM) **|** Endpoint Security (EDR/IDS/IPS/NGAV) **|** Security Awareness