

# Dwayne Robinson

747-477-4803 – dwayne@dwaynerobinson.com

---

## Executive Profile:

Self-motivated seasoned executive with expertise in the information technology sector focusing on global policy, infrastructure design, and security with cyber risk management for global enterprises. Proficient in developing and implementing significant policies and procedures that maintain global security compliance and protect intellectual property and assets within the organization. Negotiate vendor contracts focusing on achieving financial goals and sustaining organizational profitability. Strategize with the board of directors to analyze and mitigate global information technology risks and cyber threats throughout the environment.

## Professional Experience

Hollywood Park Management / Sofi Stadium

Inglewood, Ca (5/2023 – Present)

### **Head of Cybersecurity**

- Actively forging strategic alliances with legal teams to embed advanced security controls in vendor contracts, ensuring the global integrity and safety of digital and physical assets in high-profile, highly trafficked public entertainment environments.
- Redefining HWPs technology landscape by actively incorporating next-gen cybersecurity technologies utilizing Artificial Intelligence, significantly enhancing our defense mechanisms against evolving cyber threats in the sports and entertainment sector.
- Spearheading the deployment of predictive analytics for cyber threat detection, actively setting a new standard in proactive security measures for large-scale sports and entertainment venues.
- Implemented a suite of cybersecurity & overall technology policies, actively establishing benchmarks for operational rules and standards within the organization.
- Orchestrating the development of a robust incident response plan based on NIST protocols, ensuring swift and effective action against cybersecurity incidents to safeguard our global brand endpoints, infrastructure, clientele, and guests.
- Established a cybersecurity consortium to promote an organization-wide security culture, ensuring every team member, from executives to front-line staff, is actively advocating in our cybersecurity framework.
- Automating key cybersecurity processes to enhance the efficiency and accuracy of our threat detection and response capabilities, crucial for maintaining the uninterrupted operation of global events.
- Implementing a comprehensive Zero Trust architecture (ZPA and ZIA) to actively reduce reliance on traditional VPNs, fortifying our defenses and ensuring the security of digital interactions among employees and partners.
- Developed company-wide strategy to actively cultivate cybersecurity synergies, breaking down silos and integrating security practices into every aspect of our operations, from dev-ops, procurement, ticketing to live event operations.
- Increased visibility of uncategorized assess in the organization by 17%, decreases spam volume reaching users mailboxes by 33% and increased visibility of our GCP and on prem virtual environment due to the alignment and implementation of new strategic tools implemented throughout the infrastructure.

Trader Joe's

### **Chief Information Security Officer**

Monrovia, CA (05/2022 – 10/2022)

- Led the Cyber Security infrastructure for an organization of 550+ sites, 50,000+ employees, and more than \$20bn in revenue.
- Developed a team to implement a comprehensive information security program that included risk management, data privacy, incident response, vendor management, access control, network security, web application security, and infrastructure hardening.
- Reviewed SOX reports from potential vendors to determine compliance before integration.
- Executed overall company risk matrix to identify risks facing the organization and ensure tools & services are appropriately aligned to guarantee high availability and resiliency.
- Investigate, gather, and document a complete audit trail to analyze external & internal security incidents.
- Understanding and compliance knowledge of relevant legal and regulatory requirements, such as Payment Card Industry/Data Security Standard (PCI DSS) and California Consumer Privacy Act (CCPA).
- Reviewed mission-critical cybersecurity technologies, such as EDR, antivirus, firewalls, VPN, secure email gateway, Identity Access Management, Privileged Access Management, and DLP systems to develop a plan to mature the security profile.
- Manage strategic partners supporting the security operations, email security, data security/analytics, and device management throughout the organization.
- Commissioned routine security assessments on internal systems and external partners to determine an acceptable level of risk and implement tools to mitigate risk outside of acceptable tolerances.
- Provided cyber risk education and training to company employees and partners to proactively educate the team on understanding and identifying cyber risks and threats.

## Universal Music Group (UMG)

### Global Director Recorded Music & Supply Chain Cyber Security

Woodland Hills, CA (09/2017 - 05/2022)

- Established a team to monitor and remediate illicit cyber activities against the company's vast trademark and intellectual property catalog.
- Provided technical direction and leadership to industry stakeholders to minimize cyber threats.
- Implemented a strategic global intelligence program to automate the detection of cyber threats and vulnerabilities to protect the organization from cyber threats.
- Worked with partners to develop cyber security programs to dynamically identify, log and alert on cyber threats against UMG recording artists and executive management and developed protection methods against newly identified exploits.
- Devise, implement and audit global information security policies, procedures, and controls to ensure that corporate digital assets are monitored, and cyber violations are immediately addressed.
- Established a global compliance program to comply with local laws and direct routine security audits to ensure enforcement.
- Established a companywide cyber security awareness program to minimize internal threats to the organization.
- Crafted and implemented Cyber Security measures for the company's global physical and digital supply chain to reduce leaks and protect assets and media from inception to the time of official release.
- Developed and implemented vulnerability audits and penetration tests against company assets, partner companies, and sub-entities. Analyzed outcomes and devised remediation schedules to coincide with board directives.
- Devised client identity/access management to minimize unauthorized misuse of UMG personnel's likeness and reputation globally.
- Conduct cyber resiliency audits of standard platforms such as AWS, Azure, and Google Cloud to determine and mitigate risks to the organization.
- Provide briefings for the executive board of directors regarding investigations after incidents, including impact analysis and recommendations for avoiding similar vulnerabilities.

### Vice President Information Technology - Interscope Geffen A&M

Santa Monica, CA (05/2014 - 09/2017)

Directed all areas of Information Technology and Information Security across multiple channels within the organization. Managed internal systems and networks for offices in Los Angeles and New York and remote users nationwide. Collaborated with stakeholders to produce a roadmap for organizational developments and cyber threat intelligence to promote growth and infrastructure resiliency. Conducted audit investigations to identify external cyber threats and intrusions and established security protocols and policies across the organization to limit and prevent cyber theft.

- Led a team of 17 support personnel, engineers, and technical designers to implement an advanced network infrastructure to support organizational goals successfully.
- Decreased budgetary spending by 20% by reducing obsolete systems and leveraging SaaS products where appropriate.
- Increased staff productivity with proprietary mobile app and application designs which enabled increased collaboration and provided a quicker than expected ROI.
- Strategize with the executive board to develop and implement Information Technology solutions for productivity and cost-saving initiatives.
- Managed a multi-million-dollar budget for infrastructure site development, security posture, and growth.
- Engineered and implemented technical systems and tools to protect intellectual property stored and transmitted digitally throughout the organization and to external partners.
- Deployed multiple secure Intranets and Extranets across the organization to streamline approvals and secure delivery of proprietary assets to reduce expenditures.
- Executed companywide digital repository of assets to reduce shipping and offsite storage expense of assets.

### Prior Positions

Interscope Records – Senior Director of Information Technology

Santa Monica, CA (08/2003 – 05/2014)

MCA Records – Associate Director of Information Technology

Universal City, CA (2001 - 2003)

Universal Music Group – Senior Executive Support

Universal City, CA (1997 - 2001)

U-Haul International – Senior Technical Analyst / Information Technology

Phoenix, AZ (1995 - 1997)

U-Haul Company of Van Nuys – Senior Staff / Information Technology Executive

Van Nuys, CA (1988 - 1995)

## **CONSULTING**

- Advise principal partners on cyber proactive techniques to promote security and infrastructure stability for the organization.
- Identify employee exposure and implement encryption and recovery platform for protection of digital assets.
- Oversee office construction and implementation of network & server infrastructure, server, VOIP telephony design.
- Advisor to the board of directors on the global technology landscape, cyber sector, website, and corporate digital security.
- Design, implement, maintain secure infrastructure for statistical feeds to web and media partners.
- principal partners in global technology governance, GDPR
- Design and Implement cloud infrastructure for secure collaboration of music and digital assets among partners.
- Guidance on Merger and Acquisition activities specializing in technology, digital assets, and cyber threats.
- Ongoing advisory on Cyber landscape, threats, and mitigation techniques for protection of intellectual property.
- Expert guidance on SOX, GDPR, Data Privacy & Cyber Security and Ransomware prevention
- Budgetary guidance on technology systems and software.

Industries consulted for: Film & TV, Sports and Entertainment, Financial Services & Entrepreneurial

## **EDUCATION**

University of Southern California  
University of Southern California  
Florida Institute of Technology

Master of Cyber Security Engineering	2019 - 2021
Master of Business Administration	2015 - 2019
Bachelor of Science Computer Information Systems	2011 - 2015
Minor, Human Resource Management	
Magna Cum Laude	

## **PROFESSIONAL CERTIFICATIONS**

ISC<sup>2</sup>  
Microsoft  
Microsoft

Certified Information Systems Security Professional (CISSP)  
Microsoft Certified Professional  
Microsoft Certified Systems Administrator