CONTACT PROFILE REPORT

Ricky Arora

NAME
Ricky Arora

EMAIL
rikarora@googlemail.com

ENGAGEMENT
Qualys TotalCloud Cloud Sec

TITLE AND COMPANY
Director of Security Architecture · Liberty Global

PROFESSIONAL PROFILE
https://www.linkedin.com/in/ricky-arora-profile/

USE CASE
Marketing & Sales

Inferred Personality Type: Type 3 — Performer

Engagement Alignment

Dimension	Assessment	Rationale
Role Match	Strong	As Director of Security Architecture, Ricky holds a senior leadership position directly responsible for security strategy and architecture consistent with campaign targeting senior technology and security leaders.
Level Match	Strong	Senior director level aligns with the intended audience of CISOs, VPs, and Directors, confirming the appropriateness of engagement.
Subject-Area Match	Strong	Expertise includes cloud security architecture, identity and access management, vulnerability management, and security monitoring relevant to cloud and application security.
Need for Marketing & Sales	Moderate	Liberty Global’s extensive cloud and AI initiatives, combined with a risk-based cybersecurity program and evolving security strategy, indicate a relevant opportunity. However, no explicit current procurement intent is visible, so discovery-focused outreach is recommended.

ALIGNMENT STRENGTHS

- Senior leadership role directly aligned with security architecture and strategy.
- Broad, proven experience in cloud security and enterprise security architecture.
- Strong governance and transformation leadership consistent with campaign direction.
- Engagement in high-scale multi-cloud environments relevant to cloud security visibility and remediation.

ALIGNMENT GAPS

- No explicit documented current project or procurement intent for Qualys or similar solutions.
- Limited public evidence of direct involvement in container security or application security tooling.
- No confirmed ownership details for security tooling purchase decisions.

BUYING INFLUENCE

SECURITY ARCHITECTURE LEADERSHIP

Leads key strategic security initiatives influencing control strategy and architecture design across Liberty Global’s subsidiaries and portfolios, enabling decision-making for security frameworks and standards.

Evidence: Experience as Director of Security Architecture managing cloud and infrastructure security architectures and design assurance.

SECURITY GOVERNANCE AND RISK MANAGEMENT

Influences security governance and risk management practices through leadership roles and advisory positions in external security standard bodies like CSA.

Evidence: Co-author of CCMv4 Cloud Security standard and Enterprise Advisory Board member for CSA, indicating thought leadership and influence.

Professional Context

ROLE AND RESPONSIBILITY CONTEXT

DIRECTOR OF SECURITY ARCHITECTURE AT LIBERTY GLOBAL

Leads a geographically dispersed team responsible for cyber security strategy, architecture, and design across Liberty Global and its subsidiaries. Oversees strategic security initiatives to implement an integrated control landscape spanning IT, network, and multi-cloud environments including AWS, GCP, OCI, and Azure. Accountable for ensuring security architecture compliance in all programs and projects.

Evidence: LinkedIn experience details highlight leadership over global security architects managing identity and access, privileged access, network security (NIDS/NIPS/WAF), endpoint protection, cloud posture and workload protection, vulnerability management, and security monitoring.

SECURITY TRANSFORMATION LEADERSHIP AT 6POINT6

Directed multimillion-pound security transformation initiatives for diverse clients, building enduring cybersecurity functions encompassing strategy, architecture, governance, design assurance, and risk management. Accountable for Security Architecture, Information Assurance, and Security Operations teams.

Evidence: Experience record describes leadership in building and maturing enterprise-wide security governance and risk management at 6point6.

SKILLS AND EXPERTISE

CYBERSECURITY STRATEGY AND ARCHITECTURE

Demonstrates deep expertise in developing digital technology strategies and transformational security architectures across cyber security, application, and infrastructure domains. Proficient in integrating security practices within complex matrix organizations.

Evidence: Profile about section and experience at Liberty Global and BP highlight strategic security roadmap development, architecture design, and technology strategy.

CLOUD SECURITY AND MULTI-CLOUD PLATFORMS

Well-versed in securing cloud environments across major platforms such as AWS, Azure, and Google Cloud Platform. Manages cloud security capabilities including Identity and Access Management, Privileged Access Management, Cloud Posture Management, and Cloud Workload Protection.

Evidence: Experience leading security architecture covering multi-cloud environments (AWS, GCP, OCI, Azure) and involvement in Cloud Security Alliance advisory board and CCMv4 standard co-authorship.

LEADERSHIP AND TEAM MANAGEMENT

Strong leadership skills proven by managing geographically dispersed global teams and organizing cross-functional groups. Skilled in stakeholder management, mentoring, and driving performance in complex security programs.

Evidence: Roles as Director and Engagement Director include managing security architects, teams, and delivering training and briefings to global architecture communities.

RISK MANAGEMENT AND SECURITY GOVERNANCE

Expertise in cybersecurity risk identification, management, and integrating security governance into enterprise architecture and operational practices. Supports agile delivery and continuous improvement avenues.

Evidence: Experience records at BP include leading IT and OT security strategies, risk assurance, security governance, and agile coaching.

POTENTIAL BUSINESS PRIORITIES

IMPLEMENT INTEGRATED SECURITY CONTROLS

Priority is to establish and maintain an integrated landscape of security controls and architecture that covers IT infrastructure, network, and multi-cloud environments effectively to protect enterprise assets.

Evidence: Current role description at Liberty Global highlights focus on realizing a modern integrated control landscape across various technology stacks and cloud environments.

ENSURE COMPLIANCE AND DESIGN ASSURANCE

Focus on achieving compliance with secure design patterns and technical security requirements in all infrastructure and application projects.

Evidence: Responsibility for security architecture and design assurance for all programs and projects as stated in Liberty Global experience.

DRIVE SECURITY TRANSFORMATION AND GOVERNANCE

Lead transformational initiatives to mature cybersecurity functions, enhancing security governance and risk management capabilities across organizations.

Evidence: Role at 6point6 and BP include defining and leading security transformation initiatives and governance development.

ADOPT AGILE AND COLLABORATIVE PRACTICES

Embraces agile delivery methodologies and fosters collaboration among teams to deliver incremental business value aligned with strategic security objectives.

Evidence: Experience indicates championing Agile delivery, coaching teams on ceremonies and promoting cross-team collaboration.

Communication Profile

OBSERVABLE ENGAGEMENT SIGNALS

PUBLIC CAREER MOVEMENT AND RECOGNITION

Publicly acknowledged for successful security leadership and transformation work, receiving recognition from executive leaders, indicating a reputation for delivery and outcomes.

Evidence: LinkedIn post references a personal thank you message from BP's CEO acknowledging contribution to improved security posture and agility.

ENGAGEMENT PREFERENCES

SUMMARY OVER DETAIL

Prefers concise, results-oriented communication with emphasis on actionable outcomes and performance rather than extensive narrative or theoretical discussion.

Evidence: Personality context indicates preference for efficient, goal-focused communication avoiding unnecessary detail.

EXAMPLES AND CONCEPTS

Favors practical examples and clearly defined success criteria when engaging in discussions or recommendations.

Evidence: Personality guide suggests structuring prompts with goals, methods, outputs, and guardrails for clarity and effectiveness.

EVIDENCE AND NARRATIVE BALANCE

Engages best when communications provide a balance of evidence-backed insights with concise narrative focused on results.

Evidence: Demonstrated by leadership roles requiring strategic communication and reporting to executive teams.

STRUCTURED OVER EXPLORATORY

Prefers structured presentations with clear goals and performance metrics rather than open-ended exploratory discussions.

Evidence: Personality guide's recommendation for structured, efficient communication aligned with leadership decision-making roles.

DISCUSSION AND REVIEW

Values constructive review and discussion centered on achieving momentum and measurable progress.

Evidence: Leadership experience managing teams and initiatives involving collaborative governance and improvement cycles.

ENGAGEMENT DRIVERS

ACHIEVEMENT AND SUCCESS

Driven by accomplishments, delivering results efficiently and leading successful security transformations reflecting high professional standards.

Evidence: Personality self-perception emphasizes identity linked to performance, success, and leadership.

EFFICIENCY AND MOMENTUM

Seeks to achieve objectives rapidly with minimal delay, preferring clear and efficient progress pathways.

Evidence: Personality and role descriptions stress bias for short-term action and overcoming obstacles to get things done.

DECISION-MAKING STYLE

RESULTS-FOCUSED AND STRATEGIC

Combines strategic thinking with a bias towards tangible results and pragmatic action plans to achieve business and security goals.

Evidence: Profile overview describes being a technically curious strategic thinker with emphasis on short-term action.

COLLABORATIVE LEADERSHIP

Leads cross-functional teams and governance bodies, incorporating stakeholder perspectives to inform security decisions.

Evidence: Experience leading global teams and advisory board participation indicates collaborative approach.

PREFERRED COMMUNICATION STYLE

PROFESSIONAL AND DIRECT

Communicates confidently and professionally, focusing on clear, concise dialogue and avoiding emotional or verbose language.

Evidence: Personality guide recommends professional, confident, and direct tone without overemotional or verbose content.

RECOMMENDED ENGAGEMENT APPROACH

- Use concise and outcome-driven communication highlighting success and efficient security risk reduction.
- Lead with discovery questions on cloud and container security visibility, prioritization, and remediation ownership between security and engineering teams.
- Frame discussions around enhancing security control governance to support scalable AI and cloud adoption in Liberty Global's multi-cloud environment.
- Emphasize practical benefits such as workload prioritization, remediation acceleration, and cross-team collaboration without naming competitors.
- Offer actionable insights supported by metrics or relevant examples to align with leadership’s results-oriented style.
- Maintain a professional and consultative tone focused on achieving tangible security improvements aligned with business objectives.

DISCOVERY QUESTIONS

1. How does Liberty Global currently gain visibility into risks across its multi-cloud and application environments?
2. What approaches are used to prioritize cloud and application security findings to focus on the highest-impact risks?
3. How do security and engineering teams coordinate remediation ownership and workflows in your distributed environment?
4. What challenges exist in early detection of security issues during application development and deployment?
5. How does Liberty Global ensure compliance and auditability across its cloud and network security controls?
6. What goals does Liberty Global have for scaling AI-driven operations securely while maintaining governance and efficiency?

CONSEQUENCES OF INACTION

- Failure to unify cloud security visibility and risk prioritization could delay transformative AI and cloud initiatives.
- Inconsistent remediation ownership may extend vulnerability exposure and complicate security governance across subsidiaries.
- Insufficient integrated controls could increase exposure to evolving cyber threats impacting critical telecommunications infrastructure.
- Lack of scalable AI governance may introduce operational risk and hinder autonomous network operations.
- Inefficient collaboration between security and engineering could dilute accountability and slow down mitigation efforts.