Albert HUI

+852 9814 3692 | albert@securityronin.com | 16/F, Nexxus Building, Central, Hong Kong

Risk Advisor | vCISO | Digital Forensics & Fraud Investigator

Proven stakeholder management & communications. Ongoing dialogs with regulators.

People person with deep tech knowledge – high court-approved forensics expert witness & ex-HSBC incident response lead.

Adept in explaining tech risk in business language thereby getting diverse stakeholders on to the same page so projects can move quickly: consulting clients range from critical infrastructure utility groups, space industry, large conglomerates, to international hotel chains, across multiple countries (including India, Indonesia, Australia, and China). Consulted by HKMA, consultative inputs incorporated into MAS guidelines. $(ISC)^2$ InfoSec Leadership Achievements Honouree.

SIGNATURE ACHIEVEMENTS

- ✓ Stakeholder expectation alignment for a 5-year ICT infrastructure uplift program at a world-class racing club.
- ✓ Security architect of a now-licensed crypto exchange, co-designed the original security architecture & technology stack.
- ✓ Improved group-wide incident response playbook (particularly against malware) for a top-tier investment bank.
- ✓ Big 4 directorship on smart city critical infrastructure IoT security assurance consulting.

WORK EXPERIENCE

Concordium, London | **Security Consultant** **Jul 2025 – present**

Concordium is a pioneer in achieving regulatory compliance while preserving privacy, via ZKP (zero-knowledge proof) algorithms. Riding on my experience designing security architecture and controls for crypto asset exchange, provide assessment and advisory to envelope-pushing innovative web3 systems.

- Brought DevSecOps (development, security, and operations) up the maturity curve focusing on CI/CD (continuous integration / continuous delivery) pipeline, supply chain security assurance, build artifact provenance, SAST / IAST / RASP (static application security testing, interactive application security testing, runtime application self-protection). Work closely with SRE (software reliability engineering).
- Advised on end-to-end security architecture, from UI/UX (user interface / user experience) to multi-signature custodianship, to attack surface management.

Blackpanda, Singapore | **Incident Response Specialist** **May 2025 – present**

Responsible for practice improvement initiatives:

- Extended delivery scope through integrating Blackpanda's technical incident response practice with my forensic expert witness expertise, actualizing expert reports and reporting narratives that are courtroom and boardroom ready.
- Incident response process reengineering. Improved triage efficiency by 60% through better tooling (integration of off-the-shelf (commercial and FOSS) software, special purpose tools, and in-house developed software (I am a Python, Rust, and Linux kernel developer with software listed on official repositories)) and process improvement.

Institute of Directors (IoD), London | **Cyber Security Advisor** **Jul 2024 – present**

Directors are increasingly charged with oversight responsibilities across many areas, not least cyber risk, which in this age of double extortion ransomware can easily escalate into existential threats to the organization. Took office to provide practical guidance and strategic risk advices to directors so they may better fulfill fiduciary duties.

Telstra, Hong Kong | **Principal Consultant, Cyber Security** **Mar 2023 – Jun 2024**

Tasked with developing security consulting (distinct from existing VAR and MSS business) under a new team. Responsible for strategic planning, partnership design, and pre-sales enablement & support.

- Designed, led, analyzed, and reported (end-to-end repeatable new business offering) **incident response tabletop exercise** for a large conglomerate, thereby assisted its Group CEO sending the message across group leaders that cyber security incidents can quickly escalate to the organization's existential crisis; as such crisis PR, narrative management, communications, legal & compliance / breach notification, and robust ICT paramount to sustainable business. The process and artifacts developed became template materials for repeated success.
- **Outsourcing scope and partnership model design** for incident response, led the development of partnership structure that ensures quality delivery while minimizing risks on the part of Telstra.

HKVAX (Hong Kong Virtual Asset Exchange), Hong Kong | **CISO (Chief Information Security Officer)** **Sep 2022 – Mar 2023**

End-to-end security consulting, from business development to security risk assessment & mitigation advisory, to security solutioning involving system integration.

- **Co-Designed virtual asset custodian system security architecture & technology stack**, ultimately leading to **operating licence**.
- **Liaised with SFC** (Securities & Futures Commission of Hong Kong), to interpret licensing requirements, drive compliance, and align expectations.

Security Ronin, Hong Kong | **Principal Consultant** **Sep 2010 – present**

End-to-end security consulting, from business development to security risk assessment & mitigation advisory, to security solutioning involving system integration.

- **Expert witness**, noteable cases:
  - Hong Kong court case HCCC63/2021: data recovery and image enhancement using artificial intelligence (AI) machine learning for criminal defence, defendant acquitted.
  - Hong Kong court case HCCC33/2020: mobile phone forensic examination for criminal defence, deep dive analysis of deleted WhatsApp messages, defendant acquitted.
  - Hong Kong court case KTCC6663/2013: video forensic examination for criminal defence, defendant acquitted
  - (Kuala Lumpur High Court case 22NCC-465-12/2014) cyber security expert witness vs. a multinational bank regarding its mishandling of a fraud case, case settled, client satisfied.

NTT (Nippon Telegraph and Telecom), Hong Kong | **Principal Consultant, Cyber Security** **Jan 2019 – Apr 2022**

Hired into Dimension Data to facilitate its transition into NTT unified business model, based on my experience handling transitional risks and politics during the ABN AMRO acquisition by RBS, ANZ, and Santander.

- **Architected total security solutions and transformation roadmaps**, from expectation alignments to gap analysis, to building PoCs (proof of concept setups consisting of hardware, software, and networking implementation), to socializing stakeholders including the c-suite, department heads, function leads, risk management functions, and vendors, to concur with a unified vision and project plan, leading to quickly setting in motion transformation executions.
- **Designed a practical interpretation of ZTA (zero-trust architecture)** to gain internal alignment regarding implementation playbook, engineering and management tradeoffs with rationale, particularly geared towards migrating applications to cloud.

Deloitte, Hong Kong | **Director, Risk Advisory** **Mar 2018 – Nov 2018**

Responsible for full-spectrum risk advisory services regarding cyber security, including but not limited to ISO27001 and SOC2 compliance, OWASP-based web site & mobile app penetration testing (audit), and security threat modeling (STRIDE / PASTA) and architecture review (SABSA). Managed a team of 6 consultants, with full people management responsibility (as for pure project delivery, usually led 2 consultants on individual projects).

- **Led penetration testing engagement toward smart city critical infrastructure security assurance**, as a director, responsible for business development, resource allocation & project planning, as well as managing the delivery.
- **Red teaming practice development**, towards which internal knowledge & skills transfer workshops were held including red team assessment of IoT systems leveraging offensive skills such as protocol analysis. Oversight and management of attack plans based on MITRE ATT&CK framework.
- **Management of a multi-country penetration testing project** for a world-class insurance group.

HSBC, Hong Kong | **Incident Response Lead** **Apr 2017 – Oct 2017**

SOC (security operations centre) L3 (level 3) IR (incident response) lead, responsible for incident response, threat hunting, and incident forensic investigation.

- **Handled day-to-day incident response operations**, devising incident response & threat hunting plans and mobilizing global resources across a follow-the-sun model, utilizing CTI (cyber threat intelligence) and malware sandboxing / analysis techniques.
- **Performance improvement** through authoring and improvement of IoC (indicator of compromise) detection and correlation rules in SIEM (security information and event management), EDR (endpoint detection and response), and XDR (extended detection and response) systems.

IBM, Hong Kong | **Global Security Architect** **Sep 2015 – Mar 2016**

Delivered end-to-end solutions utilizing technologies across the comprehensive IBM ecosystem.

- **Designed security architectures based on the SABSA model**, linking the choice of point solutions, engineering and management decisions, upward to business objectives and then on to clients' risk appetite and mission.
- Subject matter expert on IBM QRadar SIEM (security information and event management) and SOAR (security orchestration, automation and response) (later acquired by **Palo Alto Networks**).

Security Ronin, Hong Kong | **Principal Consultant** **Sep 2010 – present**

End-to-end security consulting, from business development to security risk assessment & mitigation advisory, to security solutioning involving system integration.

- Performed **cyber incident readiness and improvement roadmapping** for a regional critical infrastructure group in the energy sector with large-scale OT (operational technology) SCADA (supervisory control and data acquisition) ICS (industrial control systems), on-site assessments included operations and premises in Hong Kong, India, and Australia. Focusing on the detect and response pillars of NIST CSF (NIST Cybersecurity Framework) giving special attention to log depth (in addition to log coverage and availability) based on first-hand IR experience.
- Performed **security risk assessment and mitigation advisory** for a multinational insurance group, on-site assessments included operations and premises in Hong Kong and Indonesia.

Morgan Stanley, Hong Kong | **Associate, Computer Emergency Response Team (CERT)** **Nov 2009 – Jul 2010**

- Performed **incident response & management, and practice development**, improved group-wide global IR playbook (incident response playbook) for cyber security incidents, including external hacking attacks and insider threats. Served as SME (subject matter expert) on malware reverse engineering.

RBS, Singapore (transitioned into RBS during acquisition) | **AVP, Research and Threat Response** **Jun 2007 – Nov 2009**
ABN AMRO, Singapore | **AVP, Research, Guidance & Consulting**

- Performed **threat research & risk advisory**, developed threat models around banking operations involving technology, and authored risk advisory, security policies, and provided security controls implementation support.
- **Liaised with regulators** including MAS (Monetary Authority of Singapore), consultative feedback conceptualizing the then-emerging supply chain attack threat model accepted for inclusion in MAS Internet Banking Guideline version 3.

NCSI, Hong Kong | **Senior Consultant** **May 2006 – May 2007**

- Conducted **Security risk assessment and audit (SRAA)**, for the Hong Kong public sector, based on OGCIO G3 IT Security Guidelines, and OGCIO S17 Baseline IT Security Policy. Clients included Department of Justice (DoJ), Housing Authority (HKHA), Civil Service Bureau (CSB), and Department of Health (DH).

THOUGHT LEADERSHIP

CUHK (Chinese University of Science and Technology) **Medical School | Guest Lecturer** **Sep 2023 – present**

- **SBMS3208: Forensic Science**, on digital forensics

ACFE (Association of Certified Fraud Examiners) **| Trainer** **June 2017 – present**

- **2024: Basic Internet Domain OSINT (Open Source Intelligence) for Fraud Investigations**
- **2023: Crypto Frauds and Scams**
- **2017: The Art and Science of Cyber Forensic Collection Scoping**

ACFE (Association of Certified Fraud Examiners) **| Keynote Speaker** **2014**

Black Hat | Speaker **2013**

- **Universal DDoS Mitigation Bypass**

HKUST (Hong Kong University of Science and Technology) **| Lecturer** **2002 – 2005**

- **COMP252: Operating Systems**
- **COMP180: Computer Organization**

EDUCATION

- **Master of Philosophy** (MPhil) in **Computer Science** (by research) **1995 – 2000**
  Hong Kong University of Science and Technology (HKUST), Hong Kong
  Research area: information integrity assurance over noisy communication channels
- **Bachelor of Applied Science** (BAppSc) in **Computer Science** **1993 – 1995**
  Royal Melbourne Institute of Technology University (RMIT), Melbourne, Australia

CERTIFICATIONS

- **Cybersecurity: Managing Risk in the Information Age**
  Harvard University
- Practising Full Member of the Academy of Experts (**MAE**) #4080
- Professional Member of the Chartered Society of Forensic Sciences (**MCSFS**) #25790
- BIG Certified Cryptocurrency Investigator (Advanced Ethereum) (**CCI-E**)
- ETA Audio-Video Forensic Analyst (**AVFA**)
- ACSS **CSS** (Certified Sanctions Specialist) #59580267
- ISACA **CRISC** (Certified in Risk and Information Systems Control) #1417446 (expired)
- ISACA **CISA** (Certified Information Systems Auditor) #651512 (expired)
- ISACA **CISM** (Certified Information Security Manager) #1323694 (expired)
- SANS **GXPN** (GIAC Exploit Researcher and Advanced Penetration Tester) #95 (expired)
- SANS **GCFA** (GIAC Certified Forensic Analyst) #285
- SANS **GNFA** (GIAC Network Forensic Analyst) #27 (expired)
- SANS **GCIH** (GIAC Certified Incident Handler) #17703 (expired)
- SANS **GCIA** (GIAC Certified Intrusion Analyst) #7383 (expired)
- SANS **GREM** (GIAC Reverse Engineering Malware) #2389 (expired)
- Maven **AIRTP+** (AI Red Teaming Professional)

SKILLS

Languages	• Chinese (Cantonese/Mandarin – native), English (native)
Programming	• Python (expert – PyPI module author, published open-source tool on GitHub),
	• Full stack web app: Shadcn | React | TypeScript / JavaScript | Next.js | Vercel | Supabase
	• OS low-level kernel programing: C (expert – Black Hat presentation PoC co-author; Linux code contributor)
Data Science	• Pandas / NumPy | Seaborn / Matplotlib, R Tidyverse, Tableau
SIEM/XDR	• Yara / Sigma / Snort / Splunk / ELK rules

WORK PERMIT

- Australian citizen
- Hong Kong permanent resident