Biography

Manish Khera
Associate Partner / Executive Director

Contact information
EY Tower, 100 Adelaide St. West,
P.O. Box 1, Toronto, ON M5H 0B3

Office: +1 416 943 2134
Mobile: +1 437 998 4000
manish.khera@ca.ey.com

Education
Bachelor of Applied Science in Computer Engineering from University of Toronto

Certifications

Certified Information Systems Security Professional (CISSP ISC^2)
Certified Chief Information Security Officer (C|CISO EC-Council)

GIAC Certified Forensic Analyst (SANS GCFA)

Professional background

Manish Khera is an Associate Partner in Ernst & Young LLP's Forensic Integrity Services practice. Nationally, he leads Cyber Investigations, Digital Forensics and Fraud Data Analytics for Canada. This group assists clients in responding to, investigating and remediating cyber and security incidents, as well as investigating and solving cybercrime with a focus on strategic consulting, identification, preservation, collection, extraction of electronic records in support of litigation and investigation.

Prior to joining the firm, he was the Vice President, Chief Information Security and Privacy Officer at Sentry Investments. Manish has also led the Merchant Compliance and Data Breach Investigation team for JP Morgan Chase globally, where he oversaw complex high-profile global cyber breaches of large merchant companies involving credit card fraud within the JPMC portfolio. In several situations, Manish was injected in high profile Fortune 500 company breaches where his role was to oversee the crisis and maintain stability in the midst of newsworthy incidents. Manish has led the IT Security program at the post-breach TJX Companies, and earlier in his career, was both a computer forensic and security assessment consultant conducting complex investigations and leading both full penetration tests and vulnerability assessments.

Manish has extensive experience in credit card fraud, while investigating data breaches at JP Morgan Chase, he helped construct an early warning program whereas losses occurring at the acquiring bank's merchants were mined for data to inform the bank's fraud prevention programs.

Manish has significant expertise in responding to all forms of computer crimes, attacks and abuses. He has led as well as supported complex cyber investigations involving crisis & incident management, corporate espionage, advanced computer intrusions, denial of service, insider attacks, malware outbreaks, internet fraud and theft of trade secrets.

He is a deep expert with regards to digital forensics, windows artifact and system analysis. Conducting many investigations involving the recovery, analysis and authentication of forensic data on Windows systems, tracking specific user activity on client network's and the organization of findings for the use in incident response and internal investigations.

As a former CISO and CPO in financial services, Manish has a wealth of experience in guiding the protection of computer assets, policies, and intellectual property. He has worked in financial services environments with varied fraud detection controls and enabled the integration of programmed enforcement mechanisms to disallow the external sharing of fraud data and policies.

Manish has led a large scale Cyber incident investigation at a major US retailer whereas the adversary was able to exfiltrate 3rd party authorized gift cards. The adversary leveraged phishing, Office 365 user and admin credential compromise, and remote connection/control IT admin tools while performing anti-forensics to remove audit trails. Manish and team found the points of entry and persistence, and working with the client, methodically closed the holes and allowed for a return to business as usual while detailing a remediation plan to subvert future nefarious actors and chronicling a client/partner external report for 3rd party concerns.

Manish has also led several social engineering / business email compromise investigations at financial service firms, not for profits and mining firms involving the tracing of malicious actors through the tracking of tactics, adversary IP addresses, and malware types to understand the point of origin of attacks, motives, and lost data elements.