Comprehensive Digital Security Exposure Report

Prepared for: Colin McCabe

Tech Made Simple | [Email Obscured] | 0419 608 583 | www.mccabes.net

July 2025

Executive Summary

This report presents a structured, in-depth analysis of the digital presence, public exposure, and cyber vulnerability posture of Colin McCabe. The review synthesizes multiple input sources including social media visibility, historic breach data, platform usage patterns, and industry-specific risks.

The aim is to highlight both systemic vulnerabilities and direct exposures that may impact personal, professional, or reputational security.

Professionals like Colin, with a prominent public brand and history of executive roles in Red Hat, IBM, and AGI, require advanced digital resilience strategies due to:

- Persistent targeting by automated scraping bots
- Risk of impersonation for spear-phishing campaigns
- Residual traces in third-party aggregators

This assessment outlines actionable changes that have already been implemented and identifies outstanding improvements that would help maintain best-practice digital hygiene.

Exposure & Risk Analysis - Part 1

Colin McCabe maintains active public profiles across multiple digital platforms, each offering value to his personal brand while exposing metadata and identifiers that can be misused.

Key Platforms Monitored:

1. LinkedIn: Executive role disclosure, engagement in enterprise-focused conversations, article publication.
2. Facebook: Publicly accessible event albums, Red Hat leadership group photos, indirect tagging by others.
3. IDcrawl: Automated collection of scattered data including public appearances, employer references, and name variations.
4. MuckRack: Mistaken attribution to articles or content Colin did not produce, due to name match.
5. Podcasts: Leadership voice in Red Hat ANZ strategy, including recorded sessions that may be used by voice AI in future deepfakes.

Cybersecurity Risk Factors Identified:

- Email exposure in historical data leaks.
- Social graph visibility to adversaries.
- Publicly indexed images providing geolocation data.
- Misattributed authorship damaging thought leadership integrity.

Exposure & Risk Analysis - Part 2

Historical Data Breaches Possibly Involving Colin McCabe:

- **Optus (2022):** Phone number and name tied to email address. One of the largest in Australian telecom history.
- **Medibank (2022):** Contact data and policy metadata possibly indexed during the widespread health breach.
- **Qantas Loyalty (2023):** Booking metadata may reveal business destinations and expense habits.
- **Service NSW (2020):** Credential and form data including scanned ID references exposed.
- **Canva (2019):** Password hash exposure via shared work platform access.
- **PageUp (2018):** Job candidate record breaches from national recruitment databases.

Aggregate Observation:

A layered risk profile has emerged, where earlier breaches enable phishing, while newer social media data aids impersonation.

Summary Risk Levels:

- Account-level compromise: Moderate (MFA mitigates)
- Brand misrepresentation: High
- Phishing or spoofing via old metadata: High
- AI synthesis attacks (voice/photo): Emerging

Recommendations & Action Plan

[x] Strengthen Privacy Controls:

- Audit all public content across LinkedIn, Facebook, IDcrawl, MuckRack, etc.
- Disable platform integrations that pull data (e.g., LinkedIn Learning, Spotify connected apps).

[x] Lock Down Email and Domain Hygiene:

- Set up SPF, DKIM and DMARC on personal domains to block spoofing.
- Use custom alias addresses to track where leaks originate.

[x] Control the Narrative:

- Publish an official biography landing page that lists verified profiles only.
- Establish a Google Business card to appear first in search results.

[x] Ongoing Monitoring:

- Set alerts for new name mentions via Google Alerts.
- Schedule quarterly reviews of digital presence with a digital advisor.

Execution Timeline: Immediate application within 1-2 weeks with quarterly follow-up.

Post-Rectification Implementation Summary

After implementing the previously outlined recommendations, Colin McCabe's digital surface exposure has been notably reduced.

[x] LinkedIn now set to minimal public visibility.
[x] Facebook albums secured with friends-only permissions.
[x] All personal email addresses protected by 2FA.
[x] MuckRack and IDcrawl profiles reviewed and disputed.
[x] Conference photos tagged by others manually removed.
[x] Public contact form installed to route inquiries securely.

Colin's digital presence now aligns with common practice among senior IT and consulting executives. Residual visibility remains manageable and no active impersonation threats were detected at the time of this report.

General Reference List (including image links)

- https://www.linkedin.com/in/colinmccabe
- https://www.facebook.com/colin.mccabe
- https://www.idcrawl.com/colin-mccabe
- https://muckrack.com/colin-mccabe
- https://www.abc.net.au/listen/programs/radionational-breakfast/colin-mccabe/7835488
- https://www.insurancenews.com.au/life-insurance/australian-group-insurances-steps-up-tech-focus
- https://www.itnews.com.au/news/red-hat-teases-who-is-its-australian-cloud-customer-231930
- https://www.linkedin.com/posts/colinmccabe_think2022-activity-6943150501303623680-3d4Z
- https://www.linkedin.com/posts/colinmccabe_great-to-catch-up-with-this-bunch-of-people-activity-7004187650626617345-W6OB
- https://www.facebook.com/RedHatInc/videos/red-hat-summit-2021-june-experience/841358203454349
- https://www.facebook.com/travellingwithmyredhat/posts/2575355169433141
- https://tse2.mm.bing.net/th/id/OIP.CTXMb-OjwOf3vfYqYbAIjgHaKX
- https://tse4.mm.bing.net/th/id/OIP.650QrTFiidOITOo97DJr5wHaFj
- https://tse3.mm.bing.net/th/id/OIP.LoIquLYSsFFma08Nc_cyqQHaFj