S&P Global
Market Intelligence

Human/tech-interaction innovations balance public faces and private spaces

Analysts - Justin Lam

Publication date: Wednesday, July 2 2025

Introduction

Human/tech interaction has been identified as a center of gravity among security platforms. Each center of gravity has evolved, most recently with the opportunities and threats brought by generative AI. Enterprises balancing accessibility and privacy must mitigate data integrity attacks from adversarial GenAI. Human/tech-interaction innovations and improvements look to help improve the balance.

Data integrity attacks result in potentially greater dangers for enterprises than attacks on confidentiality or availability. These attacks are more difficult to grasp, let alone quantify. Adversarial GenAI, along with greater accessibility of key personnel, compounds existential perils for enterprises (e.g., loss of brand accessibility, enterprise trustworthiness, and safety of staff and stakeholders). This report frames broader issues between accessibility and security and recaps some human/tech-interaction (H/TI) improvements from RSAC 2025.

The Take

Data integrity — the full accuracy, reliability and consistency of data, free from corruption or alteration — is fundamental for enterprises to develop trust, privacy and safety. For enterprises, brand accessibility and trustworthy representation increasingly come from individuals representing the organization. At RSAC 2025, the balance of key executive access and executive security was in full view. Adversarial GenAI built on exposure and access from personnel creates more plausible phishing attacks and misrepresentations, and harms both the staff and the brand. Protecting the public faces of an organization and ensuring the spaces they operate in remain private will be essential for organizations growing their presence online and in the real world.

Integrity is central

The "CIA" triad consists of the security principles of data confidentiality, integrity and availability. Harms are categorized and prioritized with this triad, historically with a greater emphasis on confidentiality and a lesser emphasis on availability. Theft or exfiltration from data breaches harms data confidentiality; ransomware or denial-of-service harms availability. Attacks on data integrity, such as fraud and impersonation, result from altered or misrepresented data. Business email compromise or phishing attacks rely on plausible representations of data.

Adversaries combine and sequence attacks against all three principles. The credible phishing email (integrity) or incessant TOTP (time-based one-time password) challenges (personnel availability) may be just the first steps in an exfiltration process (confidentiality). Within enterprise risk management frameworks, priorities have been given to more quantifiable losses. The cost of confidentiality data breaches is roughly proportional to the quantities and qualities of nonpublic personal information or personally identifiable information lost. Data availability breaches cost roughly proportional to lost opportunities.

Damages to data integrity affect overall trustworthiness and may present a greater existential challenge. Business email compromise attacks could drain an enterprise's coffers. Disinformation, abuse or fraud may irreparably harm customer experience and brand. While deposit insurance exists for many banking accounts, no such protections are in place for disinformation panic or market manipulation in equity or alternative finance markets.

Enterprises must lead against attacks on data integrity. The same principles to secure data confidentiality and availability should be applied where relevant. Challenges are massive as they are subtle — there are no clear regulations or external forcing functions in many cases. Compounding the data integrity challenge, the changing presence of corporations requires accessibility, privacy and safety.

Public faces

The December 2024 fatal shooting of UnitedHealthcare CEO Brian Thompson was a topic of discussion within RSAC 2025. While the physical and information security realms have historically remained somewhat separate, the use of data security attacks to execute physical attacks has affected private enterprises.

Enterprise presence has become more digital and fragmented; individuals from enterprises are influencers, and they extend the company's brand. In efforts to be more customer-driven, enterprises showcase internal workings and personnel to add depth to their brand. Factory tours have been augmented by Reddit or podcasts. Professional service organizations display the names and appearances of their staff rosters. Millions of professionals maintain LinkedIn profiles. Participation in other formal and informal forums via Signal, WhatsApp, Slack or Discord is common. Marketing attribution increasingly stems from direct employee engagement rather than centralized corporate marketing campaigns.

Putting boundaries on this presence, data deletion firms such as DeleteMe, Optery and Redact.dev exhibited their business-to-business offerings. These data deletion solutions were originally packaged as individual subscriptions, and they automate participant opt-out and deletion requests from third-party data brokers and other organizations. Identity governance and identity provisioning offer intriguing integration or bundling options; as enterprises provision users, they will increasingly want to ensure that they directly control any identifiable information. Enterprise password manager 1Password integrates with HaveIBeenPwned to identify any accounts where usernames, passwords or other linked information have been revealed from previous data breaches.

Subsequent data integrity attacks have been subtle and profound since Thompson's death. Enterprises building their brand must face data integrity attacks of disinformation or misinformation. The volume of public discourse beyond UnitedHealthcare's control is significant, with real and generated fringes corrupting reality. The harm and abuse stemming from misinformation normalize violence. These attacks have cast fear into the public faces of the brand and driven companies to ensure their safety.

Private spaces

Executive protection that guards against data integrity attacks and physical safety attacks was on display at RSAC. BlackCloak focuses on key executive digital protection. Partnerships from Blackbird.ai and Reality Defender address the ongoing narrative attacks and deepfake attacks, respectively, that look to tarnish brands and harm key personnel.

More broadly, the combination of security for GenAI and social engineering defenses highlighted data integrity attacks. Fresh off a $35 million funding round, Doppel looks to guard against social engineering attacks by looking through multiple channels with both GenAI and human-in-the-loop analysis. Yet knowing the adversaries and the many methods they use requires more context than ever. Threat intelligence efforts mining publicly available intelligence (OSINT) have primarily focused on exposure. OSINT tools such as Shodan or Google Dorking are only the first steps to building this broader context against data integrity attacks. Identity verification services promise to be much more contextually aware, given the growing prevalence of deepfake attacks.

Existing H/TI vendors such as Proofpoint, Mimecast, Abnormal.ai, Material and KnowBe4 will continue to augment end-user awareness with greater intelligence against social engineering and deepfake attacks. Phishing identification and response is no longer just a periodic check carried out by end users, but involves the security response from all.

From a regulatory perspective, data integrity has been considered in anti-fraud and anti-money laundering use cases. Banking regulations driven by "know your customer" mandate the trustworthiness of borrowers and depositors. Other data integrity attacks against reputation, user safety or trustworthiness are less mandated by external regulation or frameworks. Digital executive protection provides an important and tangible next step. Information security has not resonated well with the C-suite staff; technology risks used to seem arcane and intangible. Now, C-level protection and data integrity are more apparent, given the convergence of the business and key personnel safety. In relief, directors and officers insurance policies and US SEC materiality may also change. D&O insurance typically provides coverage for personal liability for wrongdoing. Might more active crisis management from digital exposures affect coverage and liability? Similarly, SEC materiality has frequent addendums; changes in control are almost always material events. Potential harm is a material risk factor in filings. By maintaining a more tangible focus on executive protection, might the lessons learned be more broadly and manageably applied to the rest of the organization?

The industry recognizes harm but has difficulty defining it — and even more difficulty economically prioritizing suitable risk management. Fundamentally, enterprises will always lean into brand and business. Rewards have been prioritized over risks, as growth investments have a return on investment; risk avoidance does not. Enterprises have spent massive sums on search engine optimization and advertising to build brands. They have layered CRM, analytics, customer experience and now agentic workflows to further drive customer engagement. Tying the risks to the greater rewards will remain a fundamental challenge for H/TI vendors. The best of all worlds ensures adequate security and safety of the brand and the brand's public faces, as well as better enabling business growth. The changing landscape for enterprises to more safely promote their public faces may provide a way forward together.

Enterprises potentially face a more difficult online environment to guard against data integrity attacks. Major social media platforms from X and Meta Platforms Inc. are less neutral than ever, as they have both dismantled third-party external fact-checking and are inserting GenAI content directly into their experiences. For H/TI vendors, opportunities await. According to 451 Research's Voice of the Enterprise data, enterprises are increasing their investments in security for GenAI — the most popular increase among all technology categories. The combination of reduced or more controlled data exposure, deepfake defenses and narrative controls to deeply identify data integrity harms will be required for safe spaces.