Building a better working world

Understanding open-source intelligence (OSINT) and its value to threat monitoring and investigations

Forensic & Integrity Services

July 2023

Open-source intelligence is intelligence derived from publicly available sources. Organizations can leverage OSINT monitoring as a crucial component of their "early-warning system." OSINT can help organizations protect their personnel, property and company reputation; monitor for threats; and remain agile in today's increasingly complex threat and risk environment.

OSINT is a crucial element of an intelligence framework

OSINT monitoring is a crucial element of an organization's early-warning system in today's world.

Several global information trends, most notably the tremendous growth in the global public information dataset (including social media) and the development of increasingly sophisticated OSINT tools and practices, are combining to dramatically increase the return on investment for OSINT collection and analysis. Today's OSINT monitoring techniques and tools can survey the ever-expanding universe of public information to detect indicators of various risks and threats before they are reported in traditional media or come to the attention of regulators and internal stakeholders. OSINT analysts can deploy cutting-edge monitoring tools to design customized, risk-based queries to scrape the internet, social media and the dark web, among other sources. Properly designed, these query frameworks can give corporate decision-makers crucial time to react and avert emerging challenges and crises like misinformation campaigns, executive impersonation and insider threats.

Other more disturbing trends on the global information scene also demand increased focus on OSINT. In particular, deception strategies, enabled by new technology, are on the rise. Nation-states, criminal organizations and many other actors are leveraging synthetic information technologies (e.g., "deep fakes") that are becoming increasingly available and effective. Deep fakes enhance the effectiveness of fraud techniques like phishing and business identity compromise (BIC) because perpetrators are able to recreate a company's or executive's corporate persona with a stunning level of realism. It is increasingly possible to disrupt an organization's efforts to get its message out into the world, damaging a company's reputation. Clear and precise OSINT monitoring practices are a crucial element of the solution that organizations must deploy to discern fact from "fake" as these new deception practices become increasingly prevalent and effective.

OSINT is becoming more valuable, and more necessary, in today's world. Leaders responsible for protecting organizations' personnel, property and reputation should focusing on building out OSINT capabilities as part of a larger global, persistent monitoring capability.

Developing an OSINT monitoring function

Developing an OSINT monitoring function requires a thoughtful strategy focused on need, capability and process.

As a first step, leaders should focus on defining requirements by asking these questions:

1. What internal and external organizational risks need to be considered (e.g., cybersecurity, fraud, insider threat and geopolitical disruption)?
2. What open-source data can be mined to help us detect threats related to these risks (e.g., social media postings, chatrooms, dark web content, alternative media reporting and blogs)?
3. What resources (personnel, tools) do we already have on hand (e.g., corporate security, investigations, legal and compliance resources)?
4. What legal and regulatory issues must be addressed (e.g., privacy and data security concerns)?

With the requirements established, the next step is to build out a capability. Typically, this will mean developing a team of trained OSINT analysts and arming them with intelligence research tools and technology. Striking the correct balance between the human analytical mind and technology capabilities is crucial to success.

This capability should be integrated into an information dissemination process to help inform company decisions and get information to decision-makers. OSINT data can be shared with departments responsible for corporate security, cybersecurity, brand protection and other risks. Intelligence briefs and assessments, including OSINT and data collected through other means, must be shared up the chain of command in ways that empower leaders to make correct decisions. Those with responsibility for the intelligence process must be wary of siloed formation, which is a persistent threat to intelligence.

Contacts

Chris McCavitt
Managing Director
Business Intelligence
Ernst & Young LLP
chris.mccavitt@ey.com

Brian Wolfe
Managing Director
Crisis Management & Incident Response
Ernst & Young LLP
brian.wolfe1@ey.com

Christine St. Pierre
Manager
Business Intelligence
Ernst & Young LLP
christine.st.pierre@ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

About EY Forensic & Integrity Services
Embedding integrity into an organization's strategic vision and day-to-day operations is critical when managing complex issues of fraud, regulatory compliance, investigations and business disputes. Our international team of more than 4,000 forensic and technology professionals helps leaders balance business objectives and risks, build data-centric ethics and compliance programs, and ultimately develop a culture of integrity. We consider your distinct circumstances and needs to assemble the right multidisciplinary and culturally aligned team for you and your legal advisors. We strive to bring you the benefits of our leading technology, deep subject-matter knowledge and broad global sector experience.

SCORE No. 20424-231US
CSG No. 2305-4258140
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com/us/forensics