Constella

INTELLIGENCE INSIGHT

Protective Services in the Digital Era

Poll reveals top obstacles in providing open-source programs and digital close protection among U.K. security professionals

2022 | Survey Report

SUMMARY

Constella conducted a poll among 100 members of The Security Institute, the United Kingdom's largest professional membership body for security professionals. The results reveal key obstacles in the widespread movement toward open-source intelligence and digital close protection. Understanding the risks and setbacks associated with such frameworks is essential to successful and safe implementation.

WHAT IS "DIGITAL" CLOSE PROTECTION?

The provision of physical security with the goal of protecting an individual is known as "close protection". Now, the emergent and increasingly complex interconnections between physical and digital risk require real-time situational analysis of open-source intelligence for a holistic view of developing threats.

Some core ideas have not changed much, like advanced site-reconnaissance, movement and resource planning, principal schedule management, assessment of physical site details, distribution of individuals and the public, and other environmental considerations. However, the convergence of the digital and physical spheres makes it critical to account for the expanding range of risk factors and threat vectors that impact the implementation of any successful close protection strategy.

KEY FINDINGS

1. **More data but less resources:** Protective Services teams are generally responsible for open-source risk management.
2. **Time and complexity deter open-source intelligence implementation:** Security professionals believe open-source intelligence is too time consuming and/or too complex.
3. **The necessary transition to hybrid security:** The most significant obstacles for providing digital close protection include cost and the need for privacy.

WHY IT MATTERS

1

More data but less resources

Executives & VIPs are impacted by personal exposures, as are their family and close circle of trust, in an era of impersonation fraud and physical threat. From 'doxxing' to deepfakes, there are creative methods for threat actors to exploit people. As both VIPs and physical premises become more digitally native, a wealth of multimedia and leaked online data can be weaponised for physical or reputational attacks. Synthetic ID fraud, IP counterfeiting, account takeover, blackmail and unauthorised entry are easily achieved if trade secrets, location data, and confidential information are spilled online. The majority of Constella's poll respondents expect their organizations' Protective Services to handle open-source risks, but nearly one-third reported low bandwidth for those teams.

2

Time and complexity deter open-source intelligence implementation

Open-source intelligence is here to stay, but some security professionals face obstacles in providing it within their organizations. Constella's poll reveals time and complexity as the most significant setbacks. Nearly half of respondents believe open-source intelligence is too time consuming, and one-third do not have a clear starting point to provide it.

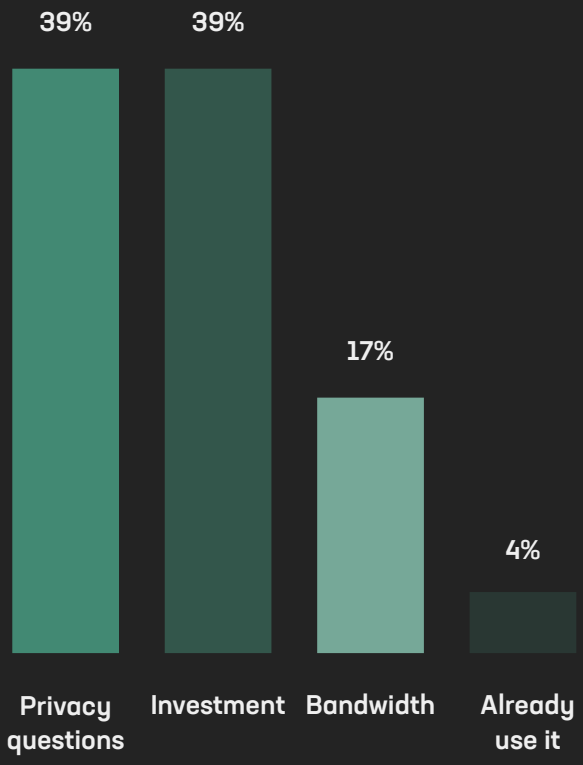
3

The necessary transition to hybrid security

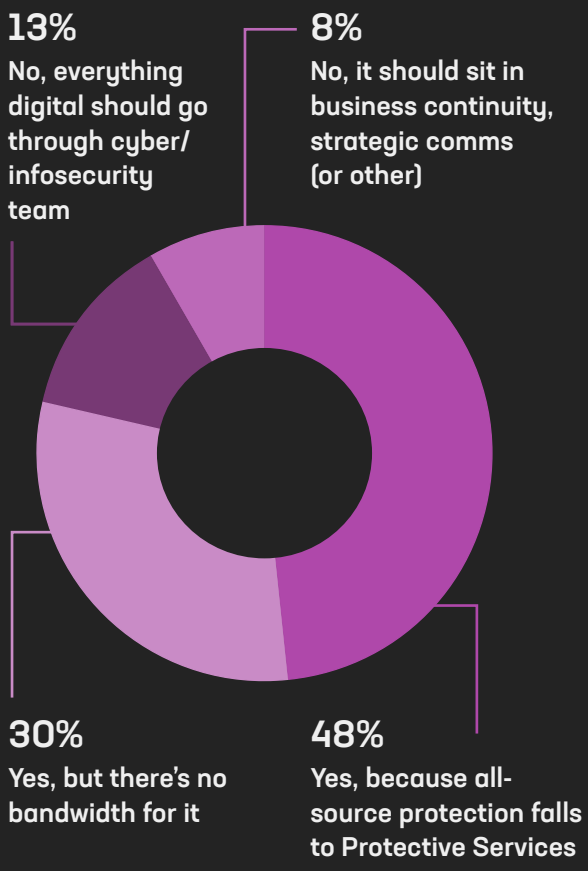
Beyond traditional close protection, and even fraud, VIPs can suffer personal brand damage thanks to misinformation and the speed and effectiveness of global public opinion. Someone can go from hero to zero with one tweet, so the reputational risk associated with a person is directly relevant to their close protection and hybrid security. However, the path to digital close protection is not perfect. Constella's poll respondents indicated investment and privacy questions as the top two blockers to achieving such protection.

SURVEY RESULTS

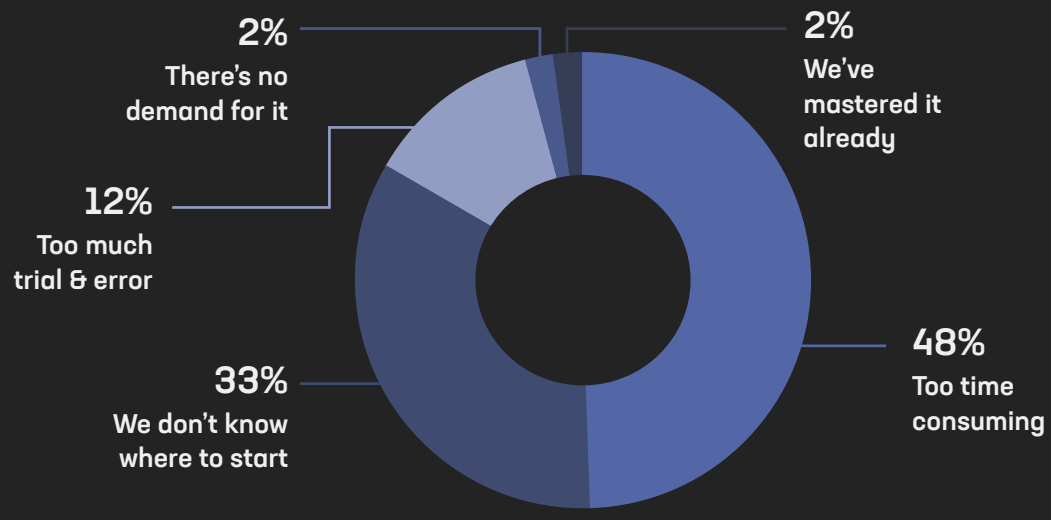
What is the biggest blocker to providing "digital" close protection?



Key asset protection: Should your organization's Protective Services manage open-source risks?



What is the biggest blocker to providing open-source intelligence, generally?



About Constella Intelligence

Constella Intelligence is a global leader in Digital Risk Protection that works in partnership with some of the world's largest organizations to defeat digital risk by identifying and monitoring potential insider threats. Our solutions are a unique combination of proprietary data, technology, and human expertise to anticipate, identify, and remediate targeted threats to your people, your brand, and your assets at scale—powered by the most extensive breach and social data collection from the surface, deep and dark web on the planet, with over 100B attributes and 45B curated identity records spanning 125 countries and 53 languages.

Our recent work has been featured in major mainstream media like the Wall Street Journal, World Economic Forum, Forbes and Krebsonsecurity.com in addition to other notable media.

To learn more about how you can proactively anticipate, identify, and remediate targeted threats to your people, your assets, and your brand try our Exposure Risk Tool to see if you or your company has been exposed - FREE.

Why Constella

OUR TEAM

We're a diverse multinational team committed to becoming the most trusted global partner for defeating digital risk. Constella integrates interdisciplinary intelligence community analysts, infosec pioneers, military veterans, and tech entrepreneurs with advanced analysis of surface, deep, and dark web to protect what matters most.

OUR INSIGHTS

Our diverse team of expert multidisciplinary cyber intelligence analysts delivers real-time, actionable insights to identify emerging threats to your organization, including insider threats and reduce risks emerging from social media, surface, deep and dark web.

OUR DIFFERENCE

Our unique technology, coupled with our world class analysts empowers advanced analysis across the entire risk surface protecting organizations, its executives and employees and their critical assets. Because, the best way to overcome future threats is by facing them today.