Securing Cryptocurrency Offices

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

Securing cryptocurrency offices from eavesdropping and espionage is a hot topic. Electronic surveillance (the spying kind) has a new target, digital assets.

You would be forgiven if you put all the blame on computer hacking. It is a common misconception. Lax security around the office and failing to conduct [Technical Surveillance Countermeasures (TSCM) inspections](https://counterespionage.com/tscm-inspection-process/)[1] precedes computer hacking. It is the reconnaissance gathered at this stage which allows some hacks to eventually happen. In the case of a crypto currency trading firm, major losses can occur without a hack.

Consider this, leaked strategy conversations can net an eavesdropper millions of dollars before the targeted trader even touches the keyboard. Bugs and other types of eavesdropping devices capture their strategies, as they speak. Valuable words and ideas are zapped away at the speed of light. The IT security folks never had a chance.

TSCM information security inspections actually take a [holistic](https://counterespionage.com/holistic-information-security/)[2] view of information security. At this level of risk multiple information loss vulnerabilities are considered. In short, TSCM is [counterespionage for the business world](https://counterespionage.com/).[3]

In addition to a trader's own crypto-assets, their clients' bespoke portfolios are also at risk. Some cryptocurrency offices also need to protect their cold storage areas. Cold storage is a temporary transfer to an offline wallet. These wallets are kept on devices such as a USB memory stick, CD, hard drive, paper, or offline computer. Then they are stored in safes or hidden locations. This is one reason why detection of covert spy cameras is part a TSCM inspection when securing cryptocurrency offices.

Traders want assurance they are not being spied upon. With crypto market capitalization reaching nearly [$2 trillion](https://www.sec.gov/Archives/edgar/data/1679788/000167978821000005/q121shareholderletter.htm)[4] recently it is no wonder. The cryptocurrencies and crypto derivatives markets are volatile enough without having to worry about financial espionage.

How to Secure a Cryptocurrency Office

1. Contact a [competent technical security consultant](https://counterespionage.com/competent-tscm-consultant/).[5]

---

[1] https://counterespionage.com/tscm-inspection-process/

[2] https://counterespionage.com/holistic-information-security/

[3] https://counterespionage.com/

[4] https://www.sec.gov/Archives/edgar/data/1679788/000167978821000005/q121shareholderletter.htm

[5] https://counterespionage.com/competent-tscm-consultant/

2. Explain your current security measures, concerns, and goals.

3. Conduct an initial TSCM inspection to benchmark the current security posture.

4. Review the findings and recommendations with your consultant.

5. Create a security remediation plan for the cryptocurrency office.

6. Conduct regular follow-up TSCM inspections to limit windows-of-vulnerability should an eavesdropping device(s) be found, and to identify new vulnerabilities.
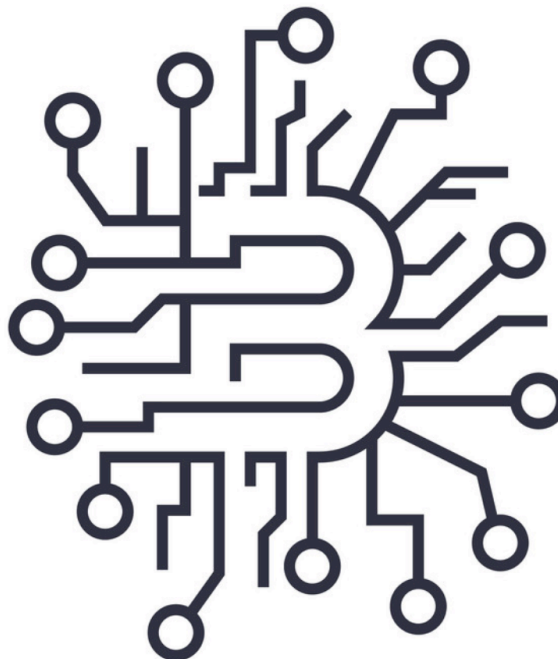
Quarterly inspections are the norm. Less sensitive areas may be scheduled on a triannual or biannual basis if the budget is limited.

Securing cryptocurrency offices with scheduled TSCM bug sweeps is rapidly becoming a standard practice. A sweep team's written report documents the effort and shows due diligence on the part of the crypto firm.

"TSCM counterespionage bug sweeps are cheap insurance. No… they are *better* than insurance. Insurance can't prevent a loss."

***

Kevin D. Murray CPP, CISM, CFE, CDPSE is a business counterespionage consultant and TSCM specialist with over four decades of experience.

Murray Associates[6] is an independent security consulting firm, providing eavesdropping detection and counterespionage services to business, government and at-risk individuals.

We began securing cryptocurrency offices and data centers[7] in 2014, and all other types of businesses since 1978.

Headquartered in the New York metropolitan area, a Murray Associates team can assist you quickly, anywhere in the United States, and internationally.

---

[6] https://counterespionage.com/about-murray-associates/electronic-eavesdropping-detection/

[7] https://counterespionage.com/it-data-center-tscm-inspections/