Incident response after a hack

Dr Alexander Ressos, TEP
Of Counsel, KGP Legal LLC
Attorney-at-Law (Switzerland and Germany), Solicitor (England & Wales and Hong Kong)

The first hours after a security incident decide whether assets are recovered and whether the firm survives the regulatory aftermath. The checklist is written for a licensed or SRO-affiliated business whose hot wallet or smart contract has been exploited. It covers the first 24 hours and points to the asset-tracing checklist for what follows.[1]

Checklist

- Activate the incident response team named in the business continuity plan and open a single incident log with timestamps.
- Contain: pause the affected smart contract if a pause function exists, revoke compromised keys, move remaining hot wallet assets to new cold storage, suspend withdrawals and deposits as needed.
- Preserve evidence: snapshot systems, preserve logs, record the attacker addresses and transaction hashes, do not wipe or rebuild compromised machines before forensic imaging.
- Engage: forensic firm, blockchain analytics provider, external counsel in each affected jurisdiction, public relations adviser.
- Notify regulators within the deadlines: FINMA under the cyber-incident rules (initial notification within 24 hours), the SRO, MAS under PSN05 (within one hour of discovery for relevant incidents), and the data protection authorities if personal data is affected.
- Notify law enforcement: cantonal police or prosecutor in Zug or Zürich, the Singapore Police Force (CAD or the Anti-Scam Command), with the transaction details and addresses.
- Notify exchanges and stablecoin issuers that may receive the stolen assets, requesting freezes, with the police report reference.
- Communicate with clients: factual, timely, consistent with regulatory notifications, without promises of compensation before the facts are known.
- Assess the client asset position: whether client or proprietary assets were taken, whether segregation survives, and whether the firm remains solvent.
- Consider the insurance notification deadlines and the policy's requirements on cooperation and consent to settlements.
- Begin the asset-tracing sequence in the next checklist.
- Record every decision and the reason for it; the regulator will ask.

Copyright © 2026 Dr Alexander Ressos, TEP – Of Counsel, KGP Legal LLC. SingaporeIQ is an information website and gives no legal advice. For Singapore law advice through KGP Legal LLC, please write to alexander.ressos@kgplegal.com.sg

Notes

1. FINMA Circular 2023/1 on operational risks and resilience and the cyber-incident reporting duty under Art. 29 para. 2 FINMASA; MAS Notice PSN05 and the Technology Risk Management Guidelines on incident reporting within one hour; see Part E, Chapter XII and Part L, Chapter VII.

Copyright © 2026 Dr Alexander Ressos, TEP – Of Counsel, KGP Legal LLC. SingaporeIQ is an information website and gives no legal advice. For Singapore law advice through KGP Legal LLC, please write to alexander.ressos@kgplegal.com.sg