CFTC Technology Advisory Committee
Cybersecurity

ANDRE McGREGOR – GLOBAL HEAD OF SECURITY | TLDR

TLDR
CAPITAL

CRYPTO HACKS

Top Cryptocurrency Exchange Hacks

More than 980,000 bitcoins have been stolen from exchanges, which would be worth more than $15 billion at then exchange rates

Mt Gox	2014	$700,000,000	(850,000 BTC)
Bitfinex	2016	$72,000,000	(120,000 BTC)
Nicehash	2017	$60,000,000	(4,000 BTC)
Coincheck	2018	$534,800,000	(523,000,000 NEM)
BitGrail	2018	$195,000,000	(17,000,000 NANO)
Coinrail	2018	$40,000,000	(Various Tokens)
Zaif	2018	$60,000,000	(5,996 BTC)

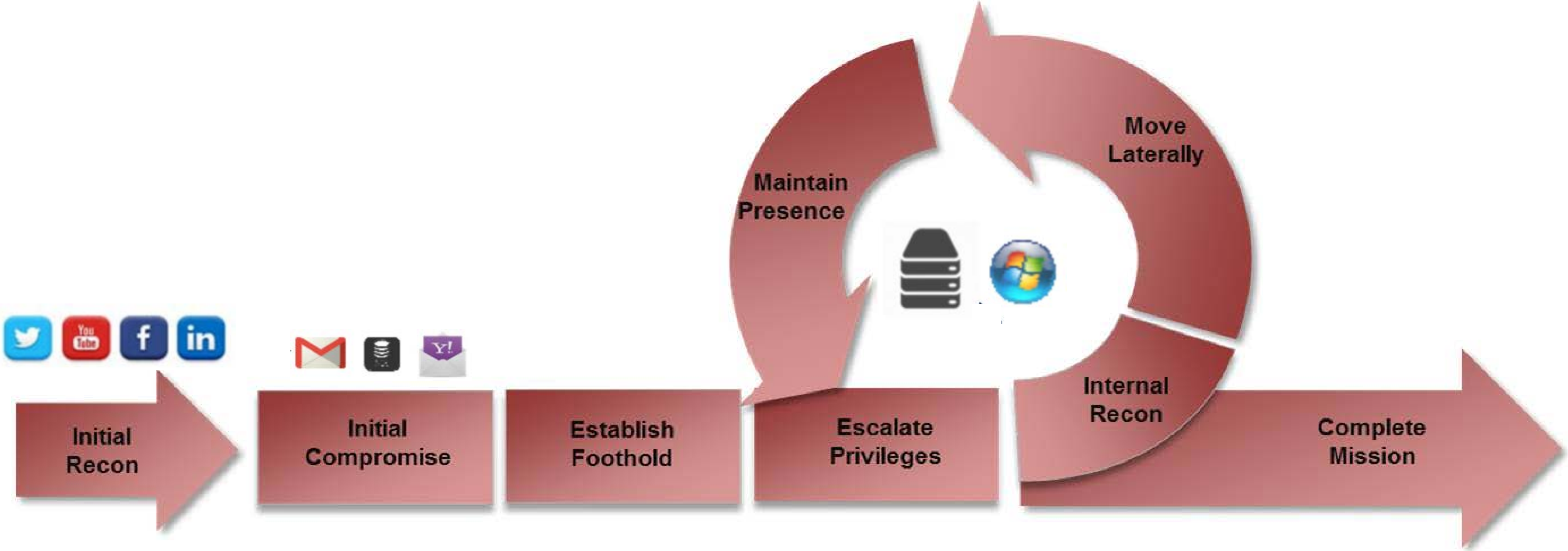
https://rados.io/list-of-documented-exchange-hacks

What Happened? Crypto Hacks Explained…

- “Employees failed to protect the private keys of its wallet where it stored all the customer's deposits”
- “Hackers sent a malicious file to exchange employees. System administrator opened the file on the machine that had access to the exchange's BTC wallet”
- “All deposits on the exchange were stored in one wallet”
- “Exchange owners filed a lawsuit against one of exchange's employees, claiming that its hack was an inside job”
- “Hackers saw the small exchange as a “ripe target” specifically for its insecure *altcoins*”

Vectors of Attack

- Email, Email, Email!
- Email is the number one threat vector for all intrusions
- 90% of intrusions still come from email attacks



DIGITAL ASSET CUSTODY

Why Custody Regulations Are Important

- Many consumers blindly trust hot wallets based on the security of a few startup founders who were thrusted into a multi-million/billion dollar company for the first time

- More savvy crypto-philes will keep a hardware wallet with them while traveling

- Then there are the scraps of paper, printouts, and polaroid cameras
  - The Winklevoss twins once cut up a paper printout of their private key to store in banks around the country

- Exchanges rotate wallets between safety deposit locations creating continuous physical risk

Custody Limitations

- Few jurisdictions have codified regulations specific to the crypto market
  - Bermuda, Jersey, Malta, Lichtenstein: Crypto friendly, mature regulations, strong financial markets, tax incentives
  - USA: Develop New Guidance or Use Existing (e.g. Financial and Segregation Interpretation No. 10 with Respect to Third Party Custodial Accounts)

- Limited standards and best practices
  - Crypto Currency Security Standard (CCSS)

- Insurance Coverage
  - Hot (Captive-Self) vs Warm (FI-Crime) vs Cold (Specie-Marine)
  - Insurance Tower Ceilings - $50m / $500m / $2bn

Traditional Insurance Risks

- Technical
  - Hacking
  - Software vulnerabilities
  - Social engineering / Impersonation

- Collusion/Counterparty
  - Third party loss of funds
  - Client fraud

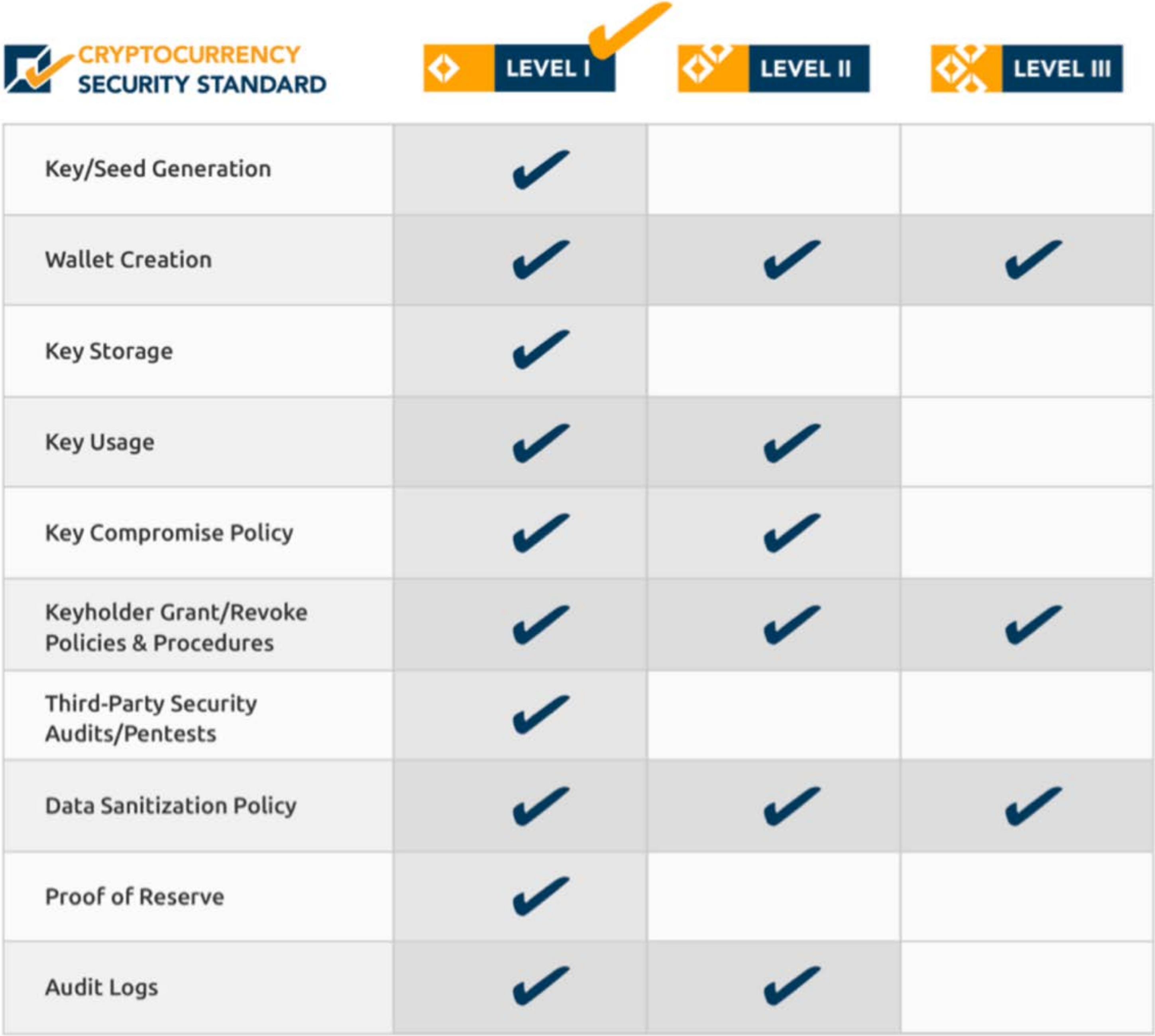
- Environmental
  - Earthquake, Flooding, Fire & other “Acts of God”

- Accidental
  - Loss of private key
  - Hardware/software failure or degradation

Crypto-specific Insurance Risks

- Private key generation, entropy, and destruction
- Supply chain security for hardware
- Pure custodian vs shared custodian
  - Multi-signature / Shamir Shared Secret sharding
- Wallet controls for transaction sizes, velocity, address whitelisting
- Source code validation and pen tests
- Storage and retrieval of backup keys (where appropriate)

CRYPTO CURRENCY SECURITY STANDARD



CRYPTOCURRENCY SECURITY STANDARD	LEVEL I	LEVEL II	LEVEL III
Key/Seed Generation	✓		
Wallet Creation	✓	✓	✓
Key Storage	✓		
Key Usage	✓	✓	
Key Compromise Policy	✓	✓	
Keyholder Grant/Revoke Policies & Procedures	✓	✓	✓
Third-Party Security Audits/Pentests	✓		
Data Sanitization Policy	✓	✓	✓
Proof of Reserve	✓		
Audit Logs	✓	✓	

https://cryptoconsortium.github.io/CCSS

Key Generation

Process	**Least Secure** ▼	**Most Secure** ▲
Key Creation	Keys are issued to the custodian by an external party	**Keys are created by the custodian themselves**
Key Creation Methodology	Unknown key creation methodology	**Key creation methodology is validated prior to use**
Deterministic Random Bit Generation (DRBG)	Keys created with non-compliant DRBG	**Keys created with NIST compliant DRBG or NRBG**
Key Entropy	Keys do not have sufficient / unknown level of entropy	**Keys are created on a system with sufficient entropy**

https://cryptoconsortium.github.io/CCSS

Wallet Creation

Process	**Least Secure** ▼	**Most Secure** ▲
Unique Address per Transaction	Wallets / Addresses are reused	**Unique addresses are generated for every transaction**
Multiple Keys for Signing	Keys have no multiple signature or sharding	**Transactions require signatures from 2 or more keys**
Redundant Key(s) for Recovery	No X of Y key redundancy	**Redundant keys are assigned for recovery purposes (e.g. 2 of 3 | 3 of 5)**
Deterministic Wallets	Wallets are not deterministic	Addresses are assigned deterministically
Geographic Distribution of Keys	All keys are in one single location	**Keys are distributed across multiple separate locations**
Organizational Distribution of Keys	All keys are with the same person or same group	**Keys are distributed across multiple organizational entities**

https://cryptoconsortium.github.io/CCSS

Key Storage

Process	**Least Secure** ▼	**Most Secure** ▲
Primary Keys Are Stored Encrypted	Keys are stored in plain text	**Key is stored with strong encryption**
Backup Key Exists	No key backups exist	**Key backup is stored in a separate location from the primary key**
Backup Key Has Environmental Protection	Backup keys are vulnerable to environmental damage or stored electronically without protection	**Key backup is protected from environmental damage including EMP**
Backup Key Is Access Controlled	Access controls are limited or non-existent	**Key backup is protected by access controls preventing unauthorized access (e.g. safe / vault)**
Backup Key Has Tamper Evident Seal	No tamper seal to identify compromise	**Key backup employs tamper-evident seal**
Backup Key Is Encrypted	Backup key is not encrypted or encrypted similar to primary key	**Key backup is stored with strong encryption equal/better than that used to protect primary key**

https://cryptoconsortium.github.io/CCSS

Key Usage

Process	**Least Secure** ▼	**Most Secure** ▲
Key Access Requires Multiple Multi-Factor Authentication	Access to key does not require sufficient factors of authentication for security	**Access to key requires an identifier and at least three: password, MFA token, in-person verification, IP whitelisting, physical key, countersigning approval**
Keys Are Only Used In A Trusted Environment	Keys are used on public/untrusted machines or in untrusted places	**Keys are only used in trusted environments**
Key Holder KYC Checks	No KYC checks are conducted on key holders	**Key holders have proper completed KYC checks**
Key Holder ID Checks	ID verification is incomplete or not established for one or more key holders	**All key holders have identity verified**
Key Holder Background Checks	Background checks are incomplete or not established for one or more key holders	**All key holders have undergone background checks**
Spends Are Verified Before Signing	No transaction verifications or whitelists are performed	Verification of fund destinations and amounts are performed prior to key usage
No Two Keys Are Used On One Device	Multiple keys for a single asset used on one device	No two keys belonging to the same wallet are present on any one device
DRBG Compliance	Signatures use a non-compliant DRBG and may have a “dirty signature” vulnerability	The ’k’ values in digital signatures are created using a NIST compliant DRBG

Key / Keyholder Grant - Revoke - Compromise Protocols

Process	**Least Secure** ▼	**Most Secure** ▲
Key Compromise Protocol	No staff has the necessary knowledge, experience, training required to rebuild keys and wallets when necessary	**Written procedures exist for each staff role to rebuild keys and wallets in order to remove risk of compromise**
Key Compromise Protocol Training & Rehearsals	No training is performed	Regular training is provided to keyholders to ensure they are prepared to invoke protocols when required
Keyholder Grant / Revoke Procedures & Checklist	No policy / procedures in place or permission changes are ad hoc through staffer with “most knowledge”	**Written procedures exist and is followed for all on/offboarding. Checklist outlines all permissions for each role in the system**
Grant / Revoke Requests Are Made Via Authenticated Communication Channels	Requests occur on multiple channels with limited verification	All grant/revoke requests are made through authenticated and authorized communication channels
Grant / Revoke Audit Trail	No audit trail	Audit trail records for every change of access including who performed the change

https://cryptoconsortium.github.io/CCSS

Operations

Process	Least Secure ▼	Most Secure ▲
Security Audit / Pen tests	No proof of a security program aligned with any cyber security frameworks	**Established security program, dedicated security staff, and external security audit conducted regularly**
Data Sanitization Exists	No sanitization is performed on decommissioned media	**Detailed policy covering sanitization requirements, procedures and validation steps for all media types**
Data Sanitization Audit Trail For Media		Audit Trails are maintained for every piece of sanitized media
Proof of Reserve Audits	No audit has been performed	**System does not hold any funds at all or ledger is public**
Application Audit Logs	No audit logs exist	**Full audit trail exists for all user/admin functions and actions**
Backup of Audit Logs		**Backups of audit data are performed regularly**

https://cryptoconsortium.github.io/CCSS

THE INSTITUTIONAL INVESTOR

The ‘Institutional’ Barrier To Entry

- ❖Institutional investors can’t enter the market without insured, qualified custodians

- ❖Insurance premiums are high and have a relatively low ceiling

- ❖Funds, exchanges and HNWIs are forced to manage their own wallets exposing risk from hackers, thieves and other criminals

- ❖No widely-recognized industry standards exist for digital asset custody

- ❖Transaction liquidity for most custodians today is quite slow

The ‘Institutional’ Solution

❖Industry standards, whether via government, consortium or SRO

❖More qualified custodians with the requisite bank-level physical, cyber, and crypto security

❖Global expansion of the regulated market

❖Robust KYC - AML - ABC process

❖Wider insurance market with continuous underwriter education

TLDR
CAPITAL

ANDRE McGREGOR – GLOBAL HEAD OF SECURITY | TLDR

@AndreOnCyber