Incident Response of Decentralized Custody; A Case Study

BGIN

Introduction

Cryptocurrency custody has become a multi-billion-dollar industry as the number of users and volume of funds continues to grow exponentially within the industry. These funds are prime targets for Ransomware and hackers alike for theft. Social Engineering remains one of the highest vectors of attacks. Custody comes in multiple forms and some individuals within cryptocurrency have funds comparable to many institutions, yet, often have less rigorous security systems in place, making them not only targets as individuals but also as attack vectors into institutions. Therefore, the individual of today has to implement cybersecurity processes and tools not unlike those of institutions.

Table of contents

1. Scope

The following document focuses on best practices within a rapidly evolving space and details a case study where Dash Core Group responded to an incident involving a cryptocurrency theft from a community member's custody. This example is discussed in the context of some best practices for individuals and institutions dealing with custody.

2. Normative reference

This document has no normative reference.

3. Terms and definitions

This document uses the following terms as the shortcut for more complete wording provided as the definition. When the term appears within this document, it should be read as being replaced by the term.

4. Abbreviations and symbols

In this document, the following abbreviations and symbols are used.

AML/CFT	Anti Money Laundering/Countering the Financing of Terrorism
BGIN	Blockchain Governance Initiative Network
BTC	Bitcoin
DCG	Dash Core Group
VASP	Virtual Asset Service Provider
PII	Personal Identifiable Information
HIPAA	Health Insurance Portability Accountability Act

NOTE: All the abbreviations SHALL appear in this clause.

5. Incident response

5.1 Responsible entities and framework

A robust security policy implemented within a cryptocurrency organization is required to minimize as well as respond to cyber incidents and threats. However, a security process can differ depending on the service, who their users are, who the victims are (internal employees/contractors or external users) and where the organization is registered.

In various countries and economic regions across the globe, regulations exist that require companies to implement certain security measures, recruit people with related experience, and in some countries, be certified that their cybersecurity meets aforementioned regulations. Although these requirements offer a standard and best practice for companies to follow, these requirements are not realistically feasible for many smaller startup ventures or cryptocurrency foundations (that are not funded by ICOs and typically non-profit) or do not have the capital to hire a dedicated security officer or a management consulting team to do a security analysis. Most of these requirements are geared towards preventing a cybersecurity incident.

However, when a Ransomware attack occurs, a response plan is required to quickly react and minimize the damage or even potentially fully remedy a Ransomware attack. Beyond that, it can even help prevent future attacks.

For a cryptocurrency foundation or organization that works on some level on the cryptocurrency protocol itself (example: Dash Core Group), the possibility for Ransomware attacks to users of the cryptocurrency itself are limited. This is due to how a cryptocurrency is structured, its limited attack points (the Network or native wallet), and how it is used. Ransomware in cryptocurrency usually targets where the cryptocurrency is as opposed to the cryptocurrency Network itself (example: Banks are targeted for theft far more than the U.S. Treasury). Some examples of targets for hackers in cryptocurrencies are: VASPS, custodians, wallets, and other places where the cryptocurrency lives. The risks are nonetheless still there for crypto foundations where foundation’s/organization’s employees are targeted. In these cases, an internal response is needed.

Potential organizational data and accounts can be compromised in several ways. If you have ever taken a cybersecurity course in healthcare, protecting HIPAA data can be a comprehensive and rigorous process. However, it matches the risks involved in healthcare. A breach of HIPAA can be catastrophic for a healthcare company. In any business, company tool service providers including (company tools, social media, work-related activities, private email accounts, gaming accounts, skype etc.) can be some potential attack vectors for hackers to steal data. Within the organization whether an internal or external threat a security task force will consist of the following individuals:

- Security Officer (if available) or train an employee (typically the COO) to manage the roles and responsibilities of a security officer.
- Affected individual—this is the individual whose account or computer has been compromised.
- Manager of the affected individual—the senior manager of the individual whose account or computer has been compromised.
- Chief Operating Officer—in the absence of the security officer, the COO creates and manages the security processes, including the response to a security attack.
- Infrastructure Team—as they are maintaining the system that was compromised, they may be able to provide several options in remedying the breach.

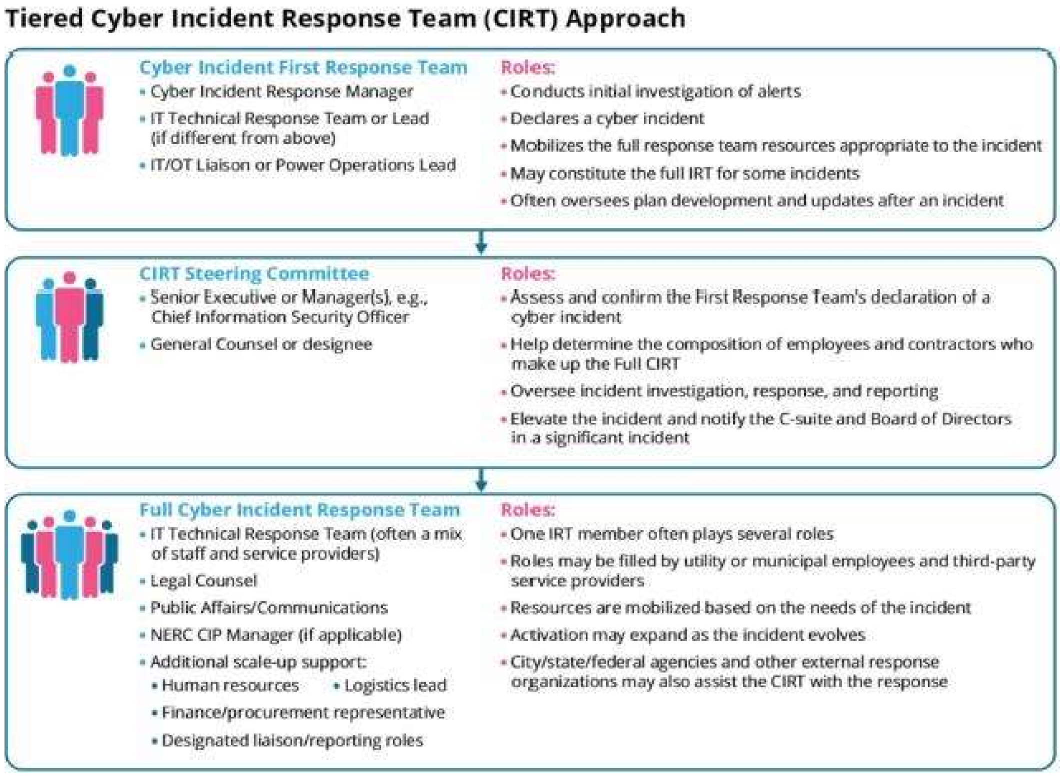
Additional Individuals

- Communications—in cases where external parties need to be communicated with
- Legal Counsel—to guide the legal side of responses and mitigate against legal ramifications of hack
- Partnership Managers—points of contact within the organization, that can assist in reaching partner services should partner systems become compromised.
- HR - Human Resources—should an HR tool or an employee be involved, support may be required from HR.
- Finance—should the incident involve payments, the attack targeted company funds, and/or support to law enforcement

Potential External Parties

- Law Enforcement—should the need arise
- Blockchain Analytics Firms—to track and trace funds paid to hackers

The first step of any cyber security preparedness and response plan is to build a response team who can immediately respond to a cyber hack. The full set of individuals selected for this team, will only be required to take action should they be required to, however the COO or Security Officer as well as Infrastructure teams will usually be the most active in cyber attacks. Others, such as those responsible for communications, will be needed should the event require external communication. Thus, it is important to evaluate your systems, teams, and processes to ensure you're not calling requesting additional support for a scenario that might only require a password change. For example, best practices suggest that a response team be split up depending on the level of severity. Below is a suggested tiered structure of what a cyber incident response task force could look like, published by the American Public Power Association.



Tiered Cyber Incident Response Team (CIRT) Approach

Cyber Incident First Response Team

- Cyber Incident Response Manager
- IT Technical Response Team or Lead (if different from above)
- IT/OT Liaison or Power Operations Lead

Roles:

- Conducts initial investigation of alerts
- Declares a cyber incident
- Mobilizes the full response team resources appropriate to the incident
- May constitute the full IRT for some incidents
- Often oversees plan development and updates after an incident

CIRT Steering Committee

- Senior Executive or Manager(s), e.g., Chief Information Security Officer
- General Counsel or designee

Roles:

- Assess and confirm the First Response Team's declaration of a cyber incident
- Help determine the composition of employees and contractors who make up the Full CIRT
- Oversee incident investigation, response, and reporting
- Elevate the incident and notify the C-suite and Board of Directors in a significant incident

Full Cyber Incident Response Team

- IT Technical Response Team (often a mix of staff and service providers)
- Legal Counsel
- Public Affairs/Communications
- NERC CIP Manager (if applicable)
- Additional scale-up support:
  - Human resources
  - Logistics lead
  - Finance/procurement representative
  - Designated liaison/reporting roles

Roles:

- One IRT member often plays several roles
- Roles may be filled by utility or municipal employees and third-party service providers
- Resources are mobilized based on the needs of the incident
- Activation may expand as the incident evolves
- City/state/federal agencies and other external response organizations may also assist the CIRT with the response

Source: https://www.cisa.gov/publication/ransomware-guide[1]

5.2 Process

As part of the preparedness process, organizations must have several ways to detect suspicious activity including system alerts, notifications from users, outages, and so on. Once an exhaustive list of potential attack vectors has been identified, create a system of alerts and a process to be alerted. At the end of the day, the first step in reacting to a security incident is detecting it.

In any institution, the employees are the most likely to be targeted. Therefore, as soon as any suspicious activity is detected either by the employee or by the security officer, the first response team (usually the security officer and infrastructure team) must get in touch with the employee and verify whether an attack has or is occurring. Once an attack is verified:

[1] Cybersecurity & Infrastructure Security Agency (CISA) & Multi-State Information Sharing and Analysis Center (MS-ISAC). (2020, September). Ransomware guide. Cybersecurity & Infrastructure Security Agency (CISA). Retrieved December 31, 2021, from https://www.cisa.gov/stopransomware/ransomware-guide

1. *Report the issue to the service provider and help them find a solution.* In many cases, the hack stems from a service the company is utilizing, such as email. Reporting the issue to the service provider takes the form of notifying them of the hack, details of the hack, and then a process of theirs to follow. This may entail locking accounts, investigations, insurance, working with law enforcement, etc.
2. *Release an internal communication* to notify employees of the attack and any necessary action required, such as backing up information, changing passwords, and other activities as needed.
3. *Investigate and identify the root-cause.* What was the cause of the hack? What was the vulnerability leveraged in the incident? Did the employee leave their laptop open at a coffee shop, or was it a malware attack due to a suspicious email file, the user downloaded? These will help towards solving the issue as well as help close future security gaps.
4. *Apply necessary workarounds and solutions.* This can vary depending on the severity of the attack, ranging from law enforcement to changing all employees' passwords.
5. *Double-check the attack vectors.* Ensure the gaps are closed.
6. *If necessary, communicate externally about the security breach*. This becomes important when the issue is expansive. For example, a sophisticated ransomware scam involved a well-known cryptocurrency cold wallet solution. Text messages were sent to owners of this product informing users that their accounts were compromised and to click links to take security measures. Unfortunately, many users fell victim to these attacks. A scaled operation such as this will require communications to external parties warning users of this scam and to not click on the link.
7. *Restore accounts and normal operations*. Once the attack has been resolved, restore accounts that have been locked. Resume normal operations with stronger security measures in place.

This overall process generally describes anytime of cybersecurity incident response process. Ransomware, like some other types of attacks, can have major ramifications and thus the details can look different depending on the context and severity. However, they can all be summed up to the above 7 steps.

There are a few things to consider with Ransomware; paying the hackers to provide you with the keys to the stolen data is expensive. In many cases where a company paid the hacker for the data to be returned, the business was able to receive the data from the hackers. In some cases, the hackers receive the payment and disappear without returning the data. However, in either eventuality, this is likely not the end of the story for the compromised business. In 68% or more Ransomware cases, the business was attacked again within 1 year of the primary incident. However, in every case, the attacks were unsuccessful because the company had learned from the previous incident, closed the security gaps, and added additional security measures such as multi-factor authentication, new password policies, and others.[2]

Many companies choose not to notify law enforcement on some cybersecurity incidents as should the incident become public, the company can incur severe reputational damage. An easy example is a cybersecurity company that has been hacked. It is recommended that law enforcement is notified in case of Ransomware, as in many cases, the data can be recovered without paying the fee, and in cases where the fee is paid, law enforcement can potentially track the movement of the funds and apprehend those responsible for the Ransomware attack.

Law enforcement does this in partnership with Blockchain Analytics Companies such as Chainalysis, BlockchainIntel, TRM, and others. These companies can trace and track the movement of cryptocurrency payments as they move from wallet to wallet, and coin, to coin. In most cases, these sophisticated analytics tools are able to even track transactions conducted by mixers/tumblers. However, as Ransomware technology and techniques evolve at a faster pace than the private sector can keep pace with Government should begin working close with the private sector, providing funding and other resources, to continue to be able to enforce current regulations.

5.3 Tracing Stolen Cryptoassets

As mentioned above, law enforcement works closely with blockchain analytics companies to track and trace suspicious and criminal transactions across multiple blockchain networks. In many cases, these companies service major cryptocurrency exchanges such as Binance, Coinbase, and others. For these VASPS to remain compliant, a robust and sophisticated system is required, given the millions of users and transactions on some of these large exchanges.

As cryptocurrency is mainly used across multiple platforms, users are most likely to be hacked through one of these services or platforms and not the cryptocurrency itself. Dash Core Group's process for theft of Dash or a ransomware attack on a partner platform, is more about collaboration and coordination than internal security measures as the vast majority of cases Dash Core Group (DCG) receives from users, relates to some social engineering tactic. DCG does not provide custodial services, nor does it sell Dash to its users, and therefore DCG is not liable for third party issues. However, users who have had their Dash stolen, reach out to DCG for help which DCG is experienced in providing. The steps taken by DCG are outlined below.

1. Once a user notifies a DCG member of the cybersecurity incident, the COO is notified of the cybersecurity incident.

[2] Palmer, D. (2020, December 8). Lightning does strike twice: If you get hacked once, you'll probably be attacked again within a year. ZDNet. Retrieved December 31, 2021, from https://www.zdnet.com/article/lightning-does-strikes-twice-if-you-get-hacked-once-youll-probably-be-attacked-again-within-a-year/

2. The partner service or platform is notified of the incident. Should the platform need assistance on a response, DCG contacts partner blockchain analytics firms as well as filing a cybercrime report to relevant law enforcement
3. Law enforcement leads investigation in collaboration with blockchain analytics who then take the process forward. DCG plays a supporting role here.

To illustrate, a retired couple and their family live in a quiet town in the U.S. They had invested in Dash during the early days of the project, and became rather successful off of the investment ($5mil+ USD). In June 2018, thieves used the elderly couple's private keys to steal Dash from their hard wallets. Following a few conversations, BlockchainIntel was brought to trace the movement of the stolen cryptocurrency.

A few months following the theft, the stolen cryptocurrency began moving to multiple wallet addresses across the world. As they moved hundreds of times, the Dash was converted into other cryptocurrencies including Bitcoin, Ethereum, and Bitcoin Cash. BlockchainIntel was able to track every transfer, which cryptocurrency, wallet address, and location. In collaboration with the FBI, BlockchainIntel traced the funds to an exchange in Asia. The FBI and BlockchainIntel were able to then determine the account owner details, including a bank account owned by the owner where the stolen funds were finally exchanged to fiat. The alleged thief was then identified the details available to law enforcement. From there, details were sent to the relevant agency in the country where the bad actor was found to be located.[3]

Though the above case is a theft and not Ransomware (where hackers were paid to return access to stolen assets), as soon as the payment has been sent to Ransomware hackers, the track and trace process for theft and Ransomware look identical in both cases.

6.Conclusion

As cryptocurrency users continue to profit from the diverse new incentives and offerings within the industry, these very same users become lucrative targets for thefts. Custody (i.e. the vault a where a user keeps their funds) must therefore be incredibly secure with security tools and processes in place even on an individual level to reduce the risk of theft. However, if, and when a theft does occur, ensuring the victim has a process to seek assistance, identify and close attack vectors, and prevent future theft is important. The lines between the individual and the institution are becoming blurred in multiple ways and individuals are the most popular vectors of attack for institutional hackers. Therefore, the processes for one may be used in the other.

[3] Hsu, K. (2020, March 27). If you have digital evidence for a theft, what's holding up Justice? BlockchainIntel. Retrieved December 31, 2021, from https://www.blockchainintel.com/blog/if-you-have-digital-evidence-for-a-theft-whats-holding-up-justice

Appendix A – Acknowledgement

(Informative)

A.1 Editors and Co-editors

- Omar Hamwi

A.2 Contributors

- Robert Weicko
- Glenn Austin

Appendix B – Informative reference

1. Hsu, K. (2020, March 27). *If you have digital evidence for a theft, what's holding up Justice?* BlockchainIntel. Retrieved December 31, 2021, from https://www.blockchainintel.com/blog/if-you-have-digital-evidence-for-a-theft-whats-holding-up-justice
2. Palmer, D. (2020, December 8). *Lightning does strike twice: If you get hacked once, you'll probably be attacked again within a year*. ZDNet. Retrieved December 31, 2021, from https://www.zdnet.com/article/lightning-does-strikes-twice-if-you-get-hacked-once-youll-probably-be-attacked-again-within-a-year/
3. Cybersecurity & Infrastructure Security Agency (CISA) & Multi-State Information Sharing and Analysis Center (MS-ISAC). (2020, September). Ransomware guide. Cybersecurity & Infrastructure Security Agency (CISA). Retrieved December 31, 2021, from https://www.cisa.gov/stopransomware/ransomware-guide