nobl.

NOBL INSURANCE REPORT U.S. CRYPTO MARKET THE HACKERS' HAVEN

HONORABLE
STRAIGHT TALKING
INSURANCE

Written by - Yvonne MCClean - Research Analyst

nobl.

ABOUT THIS REPORT

nobl Insurance has commissioned and released this research study into cryptocurrency holders in the United States. The research was carried out by cre8ive research using an online sample from P2sample with over 17 million panel members in the U.S. and powered by SurveyMonkey. It was conducted in May 2019 and revalidated in August 2019 to ensure the content is up to date. The research was carried out in an online survey questioning 1,044 U.S. residents who either own cryptocurrency (in a hot or cold wallet) or are thinking of buying in the next 12 months. The revalidation was carried out in an Omnibus phone survey questioning 1,000 U.S. residents who either own cryptocurrency (in a hot or cold wallet) or are thinking of buying in the next 12 months.

THE REPORT INCLUDES

- The key findings of the research on the on total value of cryptocurrency held in the U.S.,
- Key insights into crypto owners trust in exchanges
- U.S. crypto owners level of security awareness
- Cybercrime overview and outlook for the coming years
- The social impact and misery caused by a hack
- Commentary from a leading cyber security expert and a victim of a hack
- Innovation and strategies the crypto community could adopt to help fight cybercrime
- Conclusions and a helpful guide to help protect the crypto community online

ABOUT THE REPORTS AUTHOR & CONTRIBUTORS

- **YVONNE MCCLEAN** – Director at cre8ive.net – 30 years of providing research & insight
- **BRANDON BROWN** – Chief Executive Officer, nobl Insurance
- **GREG WIXTED** – Chief Innovation Officer, nobl Insurance
- **DR.TERRY LEE COOPER** – Global Cyber Security Expert
- **MONTY MUNFORD** – Tech Writer & Cybercrime Victim

- **THE NOBL TRUTH** – A straight talking blog and the nobl team's take on insurance

HONORABLE
STRAIGHT TALKING
INSURANCE

nobl. A FEW WORDS FROM OUR FOUNDER

In the world of cybercrime, nothing stands still for long. Since we published our first report on crypto ownership in the U.S., the latest research report from CipherTrace now suggests that global cybercrime is up 355% in the first 6 months of 2019. It's a sobering thought that they estimate outright thefts and scams are now netting criminals and fraudsters approximately $4.26bn a year.

Meanwhile, Cybersecurity Ventures predict cybercrime will cost the world in excess of $6tn annually by 2021, up from $3tn in 2015. It seems that hackers are adding, almost daily, to the tools at their service - from exit scams to ransomware payments, from SIM swapping and phishing, to taking over user accounts. These thieves are no longer content to use just one trick but are now using multiple ploys to part the unwary from their digital assets.

This flood of news from industry experts has opened my eyes to the rise and scale of cybercrime across the world. But what about the everyday crypto investor? In this, our second report, we will uncover whether US crypto owners are alert to the very real risk posed to their investments. What do they think about the threats? How much trust do they put in exchanges? We will ask a leading cyber security expert for his thoughts on current trends and future risks; including the alarming prediction that, if the current growth in hacking continues, by 2023 one third of the world's crypto market capitalization ($100bn) will have been stolen and by 2026, it will all be gone! Finally, we will look at the human impact cybercrimes have on society after individual investments have been wiped out, as it seems in many cases, at the "push of a button."

One of the more disturbing, but perhaps not surprising, findings is many smaller crypto investors are not especially concerned about security. In fact, 48% of those holding less than $1,000 lack concern that a hack will happen at all. These investors make up a significant portion of the $100bn of crypto owned in the US and could stand to lose everything should the explosion in hacking continue.

Our research also exposes that the vast majority of crypto investors have little real understanding of the scale of crypto crime. 64% either don't know how much has been hacked or believe it's a relatively modest amount of $50mn or less in the last year. When investors know the facts, they can make more informed and wise choices. As a result, our research suggests they will welcome the kind of hot wallet security that only crypto insurance can offer.

nobl. A FEW WORDS FROM OUR FOUNDER

This goes back to what I have stated in the past, mass adoption of cryptocurrency will only take place when the marketplace and investors feel safe and secure. If the hacking incidents of yesterday have taught us anything, it is that hackers will continue to follow the overflowing pool of crypto cash. With a projected average sum of $6,000 pouring into crypto per new investor in the U.S. and a projected further $74bn to be added in the next 12 months, hackers will be having a field day. There is nothing noble about cybercrime. Though some methods seem sophisticated, hackers are just common thieves whose weapon of choice is a laptop, and when hackers steal hard working people's money, that laptop can leave a trail of human misery behind.

I think this report will present our readers with the cold reality of the threats we face as a community, marketplace and society. I hope it will trigger us to make a conscious choice to do something. I believe insurance is a vital part of the solution, but also that the crypto community, insurers, exchanges, traders, cyber security experts and lawmakers, must all work together to improve security protocols and look out for each other. Otherwise, before we know it, our digital assets will be stolen right from under our noses, and only then will people wake up and say, "How did that just happen?" So, let's start to make positive change happen, right here, right now.

Feel free to reach out and connect via LinkedIn or send me an email to nobltruth@noblinsurance.com .
Join the debate on social media by using #enoughisenough

Yours truly,

Brandon

Brandon Brown
CEO and Co-Founder
nobl Insurance LLC

HONORABLE
STRAIGHT TALKING
INSURANCE

nobl.

THE TRUTH ABOUT HACKS

With so much media hype, spiralling numbers and disturbing information out there, it's hard to get a handle on the truth of what is happening today, what might happen tomorrow and what the consequences will hold for the future of crypto. To help ground speculation in some data let us start with the size of the U.S. crypto market. We have explored this both via an online panel and using best in class methodology of a telephone omnibus among a representative sample of 1002 US adults 18+.

This latest telephone survey, held in August 2019, suggests that 16 million Americans own cryptocurrency and 11.7 million are thinking of buying crypto in the next 12 months. Given an average holding of just over $6,000, this would give the US market of over $100bn, with a projection of a further $74bn added in the next 12 months. Only 10% of crypto owners hold their digital assets exclusively in a cold wallet, giving an insurable market of $90bn in the US, with an additional $67bn in the pipeline. The telephone omnibus also confirms the gender split found in our online panel research of around two thirds men holding crypto to one third women.

CipherTrace's "Q2 2019 Cryptocurrency Anti-Money Laundering (AML) Report" suggests an increase of over 300% in global cybercrime from $1.2bn to $4.26bn through misappropriated crypto investors' funds, fraudulent schemes, exit scams or hacks. If this trend continues, by 2023, one third of the world's crypto market capitalisation ($100bn) will have been stolen, enough to give a $348 to every U.S. citizen or buy Uber! At this rate, without intervention, by 2028 there would be nothing left.

ANXIOUS WHALES AND MELLOW DOLPHINS

Just how concerned are crypto investors about the security of their assets? Well, on the face of it, pretty concerned is the headline answer, with 65% of all crypto owners claiming they are very or quite concerned that their exchange will be hacked, and that they will suffer a loss. But dig beneath the surface and a more nuanced picture emerges. Not surprisingly, the 8% of our sample who hold over $50,000 in digital assets are the most nervous about hacks, with a massive 65% of these "whales" ***very concerned*** about losing their assets.

On the other hand, many of the smaller players, those with less than $1,000 of cryptocurrencies, let's call them the "dolphins" of the market, take a more relaxed attitude with nearly half (48%) neutral or positively blasé about the prospect of losing everything. It would seem the smaller investor takes a casual attitude to the risks involved, a view backed up by research carried out in 2018 among 1,000 Americans between ages 18 and 80 by Clovr, a blockchain focused research company. They reported that almost 80% of respondents considered investing in crypto as a positive form of risk-taking. However, as we will soon see, accepting the risk might be as much to do with underestimating it as with taking a philosophical approach.

nobl.

COUNTNG THE COST

While our research shows that hacking facts and figures have the power to change attitudes to crypto security, it is the human stories behind the figures that really shine a light on how crypto crimes change lives. It's not only crypto newbies that are at risk, even experienced tech expert crypto holders have fallen prey to the incredibly sophisticated, clever tricks operated by cyber criminals. Whatever you do to prevent or avert loss scenarios, hackers can strike anywhere and anytime. The dark side doesn't sleep, but grows in technologic skills and confidence, leaving victims just as damaged as if they have been mugged or burglarized. Worse, they have even less opportunity for redress. Without the protection of insurance there is no mechanism for ever seeing their investments again.

A case in point is the Cryptopia hack in February this year, which not only led to about $16mn drained in digital assets from cryptocurrency wallets, but also forced the crypto provider to move into liquidation. The liquidator, Grant Thornton's, most recent updates say there is still a long way to go until the proceedings are finished and customers can be reimbursed. So, the question is whether any of the losses have actually been recovered?

Somebody whose mind is very focused on this question is recent hack victim and tech writer for established media outlets BBC, FORBES and Telegraph, Monty Munford. Monty lost £25,000, when his cryptocurrency was stolen. Monty's experiences have left him bruised *"It's bad enough realising that somebody's nicked £25,000 of your hard-earned cash. It's even worse when you realise there's little chance of getting it back."* In a recent conversation with nobl Insurance he lays out the impact it has had on his material life and the psychological effects it has triggered: *"I am in mercenary mode and I think I've done my bit in bringing this subject the attention it deserves. .. I never used to be this man. I just want all of my money back, one way or the other."*

This is not an isolated case. There are thousands other hack victims out there who have experienced the exact same scenario. Monty Munford describes the unfolding events as follows: "When I researched the subject, there were stories of exchanges being hacked for millions of pounds and going bust, so I decided to store my assets in a wallet - myetherwallet.com. I was given two keys, one private and one public, both of 40 random numbers and letters.

COUNTNG THE COST – MONTY MUNFORD STORY

If I wanted to transfer money to my wallet, I used the public key, to access my wallet I used my private key. I was told to write down my private key and store it securely with other financial documents. I was never to reveal it to anyone or lose it. So, I printed it out, but also made the fateful decision to store it in my Gmail drafts, so I could copy and paste it when I needed to make a transaction rather than laboriously typing it out each time. I deleted my internet history after every check of my wallet for extra security. When the price of Ethereum rocketed, I was soon sitting on a decent pile of money. Then that decent pile of money disappeared. GONE IN 60 SECONDS!"

Monty continues:
"I hadn't used my private key to access my account for some time and was getting the jitters when the price of all cryptocurrencies began to fall in 2018. Maybe it was time to take some out. But when I tried to do so, I saw with horror that all of my Ethereum, about £25,000's worth, had already been taken out. The cupboard was bare. It had been moved to another private key address and there was absolutely nothing I could do about it. There seemed to be no-one to complain to."

This is a disturbing story and one that all too easily could happen to any of us in the cryptocurrency community. There are cases galore, each a little scarier than the last. There is the case of a veteran tech journalist who turned to hypnosis in order to recover $30,000 from a locked cryptocurrency device. Or the staggering $224mn lost by a crypto investor who ended up suing a large telecom provider over the loss of his fortune to sophisticated phone hacks. An inside job, as it turned out.
Monty has a view on what the industry could do better to handle such losses:

"The so-called general public are probably terrified to invest in cryptocurrencies because of such easy theft. There clearly needs to be regulation and exchanges should do more when notified of a possible theft. There should be some sort of central security regulator that victims can immediately contact, almost like an early Ombudsman, to provide some form of protection. This potential organization should be made up of all stakeholders in the crypto ecosystem from exchanges to developers"

Another interesting, but not recommendable, case of a dare going beyond a joke is publicized in Kevin Roose's report *"I dared two expert hackers to destroy my life."* The author tells the story of how he actually instigated a hack on his own personal data by some "friendly" hackers. He explains, in detail, how the story went down: *"Throughout all of this, there were vague signs that something was happening to my computer—I got more error messages than usual, and from time to time the green light next to my webcam would illuminate—but I had no idea just how extensive Dan's hack had been until I met him in Las Vegas. 'It's ridiculous,' Dan said. 'I have control of your digital life in its entirety. I have all your credentials.*

I have all your access to all your financial information, all your work information, all your personal information. I can pay people with your bank account or your Amex account.' For all intents and purposes, he said, 'I am you.' After hearing about the extent of Dan's hack, I thought about throwing my laptop into the ocean, moving to the mountains, and becoming a disconnected hermit." It clearly shows how important security is when dealing online, with the moral being take care of your data, before someone takes control of you.

nobl.

IS THE INSURANCE INDUSTRY FUELING CYBERCRIME?

A new and worrying angle on the causes of cybercrime comes from Renee Dudley, a tech reporter at ProPublica. In her article, "The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks," Renee writes *"Ransomware is proliferating across America, disabling computer systems of corporations, city governments, schools and police departments. This month, attackers seeking millions of dollars encrypted the files of 22 Texas municipalities.*

Overlooked in the ransomware spree is the role of an industry that is both fueling and benefiting from it: insurance. While insurers do not release information about ransom payments, ProPublica has found that they often accommodate attackers' demands, even when alternatives such as saved backup files may be available. [..] The FBI and security researchers say paying ransoms contributes to the profitability and spread of cybercrime and in some cases may ultimately be funding terrorist regimes.

But for insurers, it makes financial sense, industry insiders said. It holds down claim costs by avoiding expenses such as covering lost revenue from snarled services and ongoing fees for consultants aiding in data recovery. And, by rewarding hackers, it encourages more ransomware attacks, which in turn frighten more businesses and government agencies into buying policies. [..] Fabian Wosar, chief technology officer for anti-virus provider Emsisoft, said *"Cyber insurance is what's keeping ransomware alive today. It's a perverted relationship. They will pay anything, as long as it is cheaper than the loss of revenue they have to cover otherwise"*

HACKING THE HACKERS

A new approach from Dr Terry Lee Cooper, cyber security expert.

So, what is the solution to this rising tide of cybercrime? Our Chief Innovation Officer, Greg Wixted, has been in conversation with Dr. Terry Lee Cooper, who has had a distinguished career in the defence industry and at the International Atomic Energy Agency, and is now a global cyber security consultant and university lecturer in the UK. They share a joint approach, pairing a technological fight against the hackers with a global insurance solution. Dr Cooper writes:.

That if an upward trend at the brutal rate of a 300% increase per year continues then, theoretically, a staggering $12.78bn would be stolen by the end of 2020. By the end of 2021 it could rise to $38.3bn, then to an excruciating $114.9bn by the end of 2022, more than the U.S. currently holds in crypto. In real terms this would be enough to give a $348 tax rebate to every US citizen, or buy Uber!

nobl.

HACKING THE HACKERS

"In 2018, we witnessed one of the largest crypto exchange hacks globally, so far. I have just read the full report published by CipherTrace. It details the loss of over $1billion in cryptocurrencies, with Japan's Coincheck accounting for more than half, with the rest including hacks on Italy's BitGrail and South Korea's Coinrail; and of course, the demise of Cryptopia in New Zealand. These are well planned sophisticated attacks. They are happening despite even the most impenetrable technologies including those that power cryptocurrencies and blockchain. And worse yet the culprits are getting away with it. Why? Because people don't think it will happen to them.

That doesn't mean we sit back and do nothing. In my opinion, the best way to stop this modern-day crime is to understand that people need to work together. We need to unleash the power of AI just like we harnessed biometrics for border security. Let it gather, predict and detect potential threats. The technology for it already exists. Companies like CipherTrace are already using it to find ways to defeat the hackers, which is great, but how do we ingrain it into the fabric of the marketplace? We need to feed that information to many stakeholders, including those developing the risk profiles needed to cost insurance.

So, what technological defense can we mount? A paper written by three brilliant minds, Bao-sheng Wang, Wei H Tian-zuo Wang, lays out an exciting opportunity in the war-against-cyber-crime. It shows how Moving Target Defense (MTD) could alter the asymmetric situation between attacks and defences in cyber-security. MTD changes the attack surface of a protected system through dynamic shifting so it appears chaotic and changes over time. This means the work effort (cost and complexity) for the attackers to launch a successful attack will be greatly increased and the probability of successful attack decreased. MTD is not a specific approach, but an active defense principle.

It can be applied to different systems, such as IP addresses, protocols and running platforms. For example, if MTD is applied to the IP address then the IP address is mutated driving the hackers to distraction.
But could we go further? How about deploying MTD into the forecasted half a billion wearable devices that will be sold worldwide in 2021. ABI has forecasted that more than 20 million connected cars will ship with built-in software-based security technology by 2020; and Spanish telecom provider Telefonica states that by 2020 90% of cars will be online. Hundreds of thousands, and possibly millions, of people will be vulnerable to hacks via their wirelessly connected, digital devices - connected to accounts and wallets. One thing I know for sure is that not one organisation will have all the capabilities to protect them. But collectively we can unleash advanced technology, turn the tables and leave them with nothing at all - at the touch of a button!"

nobl.

FROM WEAKNESS COMES FORTH STRENGTH

The view from Greg Wixted, CIO of nobl Insurance

In 1988, Robert Tappan Morris attempted to discover the size of the web and in the process unwittingly released the world's first internet worm to spread virulently in the wild. By the time he'd realised his mistake, the Cornell University graduate student had infected 10% of the world's internet-connected computers. It was an unintended cyberattack that cost the US an estimated $10mn in damages. Fast forward to today when we have billions of devices connected to the internet. Where do we start when looking for ways to defend against cybercrime? From an innovators' point of view, we always start with the same question, "What problem are we trying to solve?" Okay, let's give it a go.

We are trying to eliminate hackers, protect our policyholders' funds and give them security and peace of mind. We need to find the flaws and vulnerabilities in our devices, not only in the ones we use today, but in the future. Future technology will be the easier one to crack as we can help develop protective features at the innovation stage. It's harder when you are looking at the many millions of devices already out there being used day in and day out. But it can be done, if, as Dr Terry Cooper puts it, we collaborate.

HARNESSING BIOMETRICS

75% of people living in the United States have experienced an online account hack. We all know how easy it is to get hold of our home wi-fi password, so one option is to turn to biometrics as a first defense. Biometric security is most often perceived in terms of authorities comparing travellers' faces to the images in their passports and other identity documents, but over the years the field of biometrics has opened up a new raft of solutions. This technology is one of the hardest forms of security to breach as it's intrinsic to a person's being. Our fingerprints and face now become the passwords using technology such as Kensington's compact VeriMark Fingerprint Key.

Behavioural biometrics is also growing based on, for example, how a person uses the keypad or app. Our unique physiological signatures can be measured in the background by cardiac-scanner biometrics – a sensor that looks at cardiac measurements, and this technology will be embedded in keyboards, mobile phones and airport scanners. These are the new technologies that can be our first line of defense in the future.

nobl.

EXPLOITING MTD TECHNOLOGY

Terry Lee Cooper has introduced the idea of MTD as another potent weapon and I would like to develop that thought. There are 2 reasons I think we should focus on this solution:

It creates a level playing field between hackers and crypto owners. If hackers don't know what IP to target, as it's shifting every few seconds, they cannot identity the hack locations from device-to-device. It becomes a games of Zig Zag. Changing the characteristics of the hack attack surface makes it very difficult for hackers to launch an attack. By increases the time it takes to launch a hack, giving more time for exchanges or law enforcement to launch AI programs that can track and hunt them down.

It's scalable. As we add 20 billion IOT devices and more exchanges it creates millions of vulnerabilities and threats that need more and more security. Because MTD makes an attack surface smaller and is shifting all the time, it essentially decreases its size, creating more efficiencies at scale.

While there are lots of benefits to implementing MTD, for it to work it must fit within the existing technology infrastructure and have little impact on the current workings of the business. It has to be simple to turn on and require minimal knowledge to manage. One new approach is to miniaturize and personalize MTD enabled devices. Whatever the way forward, one thing is clear, it has to be impenetrable; because if it leaves the back door open, we all know the hackers will find a way in and will leave the with the family silver, or in this case your crypto investments!

The US Department of Homeland Security defines Moving Target Defense (MTD) as, "the concept of controlling change across multiple system dimensions in order to increase uncertainty and apparent complexity for attackers, reduce their window of opportunity and increase the costs of their probing and attack efforts

nobl.

CONCLUSIONS

If one thing is clear from our deep dive into the world of crypto, it's that the enormous amount of assets handled by crypto exchanges makes them highly attractive to hackers. It's these hacking incidents that have helped create a negative view of crypto assets and exchanges.

To build trust, the exchanges need to adopt effective cybersecurity programs to prevent and detect external attacks. And more needs to be done in terms of due diligence regarding the source of wealth and funds. Perhaps if the media "names and shames" exchanges clearly being used for money laundering, tighter and more robust procedures will be implemented.

As custodians of the investors' assets, crypto exchanges need to do more to ensure the confidentiality and integrity of users' operational private keys. Meanwhile, the whole community needs to help educate people on how to protect themselves against hacks. This includes the media who are keen to write about a hack, but less keen on helping readers protect their accounts. With that in mind, here are some handy tips to help you keep your assets secure online:

NOBL'S GUIDE TO ONLINE PROTECTION AND SECURITY

1. **Be aware of phishing sites.** Always check whether the website address is correct.
2. **HTTPS.** Login only to secure websites with a valid HTTPS certificate.
3. **Use a secure Wi-Fi connection.** Never connect to your online wallet, exchange account or another critical security point via public Wi-Fi.
4. **Separate your funds.** Don't keep all your crypto assets in one place.
5. **Use two-factor authentication.** Always secure your accounts with 2FA.
6. **Whitelist IP and withdrawal addresses.** If you have a static IP address, use it for your safety.
7. **Double-check crypto addresses.** Some malicious programs can edit and paste a wrong transaction address whenever you send a transaction.
8. **Use security measures you can handle.** Some people never feel secure and go to the furthest lengths to secure their cryptocurrency. Strive for appropriate balance between complexity and security.

Even if both exchanges and investors implement all these measures, they may never be enough to deter every attack. The hacking industry has the incentive and the man power to stay one step ahead. This is why it is essential for the exchanges to partner with insurance companies such as nobl, to give investors peace of mind should the worst happen. In the meantime, let's keep safe and all play our part in keeping the hackers at bay now and in the future.

HONORABLE
STRAIGHT TALKING
INSURANCE

nobl.

NOBL IS A NEW TYPE OF INSURANCE COMPANY

Unlike traditional insurers, **nobl** wants everyone to share in its success. When a customer buys a policy, they become a shareholder in the company. Together, all the policyholders own the company. The administrative company receives a flat fee to run the business. So, there is no incentive to reduce or deny claims. The goal is to share the insurance company's excess surplus on an annual basis.

Founded in 2017, **nobl Insurance** has spent two years developing its first product. At product launch, it will become a U.S. regulated carrier based in the state of Michigan. **nobl** plans to launch their first product within the coming months and roll out access across the U.S. and into Europe in 2020. Other products under development are a new, affordable AI driven auto product aimed at the 225 million drivers in the United States, and a flood and crop insurance that will harness weather and satellite data to help protect the millions of families and farmers affected by floods, landslides and natural disasters every year. **nobl** is committed to creating and offering easy, simple, affordable, straight-talking insurance to everyone.

CONNECT WITH US ON

nobl.

CRYPTO

OUR VISION IS TO MAKE INSURANCE
A FORCE FOR GOOD AGAIN

WWW.NOBLINSURANCE.COM