national council of ISACS

Strengthening Cryptocurrency Regulation and Anti-Money Laundering Tools to Reduce the Impact of Ransomware

Fall 2020

The National Council of ISACS is a coordinating body designed to maximize information flow across the private sector critical infrastructures and with government.

EXECUTIVE SUMMARY

Ransomware is an extremely effective tool used by cybercriminals to illegally extort funds from consumers, businesses, nonprofits, and government organizations. The impact of ransomware is escalating at a rate that foretells a significant economic impact on global infrastructure, government entities, and the economy. Analyses by cyber experts predict an increase in ransomware activity as we see victims paying multi-million dollar ransoms, Ransomware-as-a-service (RAAS) enabling less skilled persons to increase the frequency of attacks, and new ransomware variants being unleashed to attack more operating systems and operational technology platforms. Governments across the world must ensure anti-money laundering regulations are in place and enforcement mechanisms are effectively exposing ransomware operations leveraging cryptocurrencies.

Ransomware is impacting large multi-national corporations as well as small and medium size businesses (SMBs). Well-funded and highly capable network defenders are still challenged by the many ways ransomware organizations can attack and penetrate networks. Inasmuch as best efforts to secure networks are still not preventing this criminal extortion, we must take a multi-pronged approach and concurrently attack the ransomware criminal model.

The criminal organizations running ransomware operations demand payment via cryptocurrencies. The deliberate money laundering mechanisms built into cryptocurrency ecosystems makes it difficult for law enforcement and regulatory authorities to track or seize payments. Many cryptocurrency exchanges are not governed by, nor adhering to, anti-money laundering regulations.

Analysis of ransomware payments and recent indictments indicate the criminal organizations have a Russian nexus. Russia is one of the world's countries which will not extradite its own citizens.[1] Regulatory and investigative tools have not been enhanced to enable governments to investigate ransomware cases at the speed of the internet. The bottom line is government entities and companies around the globe are paying millions in ransoms to cyber-criminal organizations primarily located outside the

1. https://www.acslaw.org/expertforum/russian-indictment-and-extradition/

victim's country. Global businesses are essentially paying a business tax to Russia and other countries which turn a blind eye to ransomware groups operating within their borders. Law enforcement from the victims' countries cannot enter Russia, and similar nations harboring these groups, to arrest the core of these criminal organizations. One avenue to disrupt these groups is to stop the ransom payments from getting to them.

Recommendations to align the regulation of cryptocurrencies with other financial instruments have predated this paper. In a paper published in March 2019 by the U.S.-based Brookings Institute,[2] Timothy G. Massad, Senior Fellow, The John F. Kennedy School of Government, Harvard University called for increased regulation ahead of a significant cyber-attack or fraud. In the year since this report, there has been an alarming spike in ransomware attacks. International governments must enact regulation and fund enforcement mechanisms now to eliminate the money laundering devices within cryptocurrency ecosystems. These many devices and schemes are detailed further in this report.

This white paper describes how criminal organizations conduct ransomware operations and their impact to society. Collectively, governments around the world must increase the regulation of cryptocurrencies. Additionally, global departments and agencies which enforce anti-money laundering (AML) regulations should be empowered and funded to better enforce AML provisions around the movement of cryptocurrency funds.

What Is Ransomware?

Ransomware is a type of malicious software cyber criminals use to attack a computer network by encrypting files on the system thus preventing users from accessing their data. The methods of access to the victim's network takes place in many ways. Typically, the attacker utilizes social engineering techniques such as phishing. Increasingly the method of attack has been the compromise of the network via a system vulnerability.

Once cybercriminals have accessed a network, one of the following paths is typically followed:

Method 1: utilize malware to immediately begin encrypting the computers on the network,

Method 2: install malware on the network which will delay encryption for a period of time which will ensure the malware has infected back up file systems, or,

Method 3: identify and exfiltrate critical data on the network, then execute either Option 1 or 2.

Once the attackers have achieved the implantation of the ransomware, theft of data, infiltration of backups, and encryption of the network, they will demand a ransom be paid. Figure 1 provides a visualization of the process. The attackers promise the key to de-encrypt the infected files in return for the ransom. Increasingly, attackers are executing Method 3, threatening to publish sensitive or proprietary data if the ransom is not paid. In some of the most recent cases, criminal organizations are demanding a ransom and then demanding a second payment in exchange for a promise from the cyber criminals to delete the stolen data.

Once the ransom is paid, the cybercriminals commonly provide the victims with the decryption keys.

2. https://www.brookings.edu/wp-content/uploads/2019/03/Economis-Studies-Timothy-Massad-Cryptocurrency-Paper.pdf

However, some victims have been known to be attacked again after they have paid the ransom and had their files restored. If the ransom demands are not met within the deadline specified in the ransom, the encrypted data remains unavailable or the data can be deleted by a wiper executable file.

It has been reported that in 2020, every attacker now typically demands a ransom be paid only in cryptocurrency.[3] This is largely because most cryptocurrencies are unregulated and cannot be traced back to the criminal organization that receives the ransom. As a result, ransomware attacks have become more successful since the ransom payment is a fungible asset.

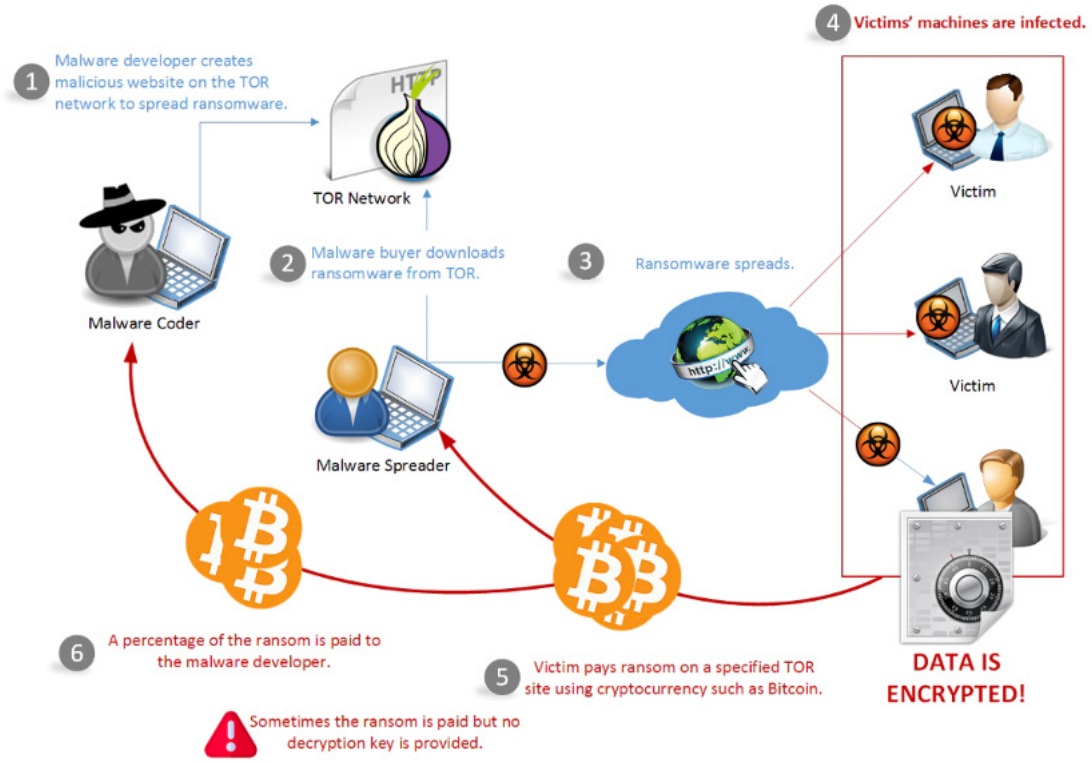

FIGURE 1: COURTESY BANK INFO SECURITY

3. https://cointelegraph.com/news/the-role-of-cryptocurrencies-in-the-rise-of-ransomware

Methods of Ransomware Infections

Ransomware is most commonly spread via social engineering through a phish with a malicious link or infected email attachment. Connecting to the link or the attachment results in the malware being launched within seconds onto the victim's computer network. The malware may be the ransomware itself or malware designed to create a backdoor for the attackers to get a foothold onto the network. Figure 2, depicts a common method used against North American victims to infect a computer network with ransomware.[4]

Other forms of entry include downloads of malicious software from accessing an infected website or by clicking on fake ads (malvertising) that can unleash the ransomware. More recently, there have been reported instances of malware being spread through texts, chat messages or even removable USB drives. Another significant attack vector for network breaches is misconfiguration.[5]

More sophisticated versions of ransomware are being created by threat actors, some of which can work without any human interaction. This more sophisticated malware is called a "drive by" attack, and this ransomware infects a system through vulnerabilities in some browser plugins or security software updates.

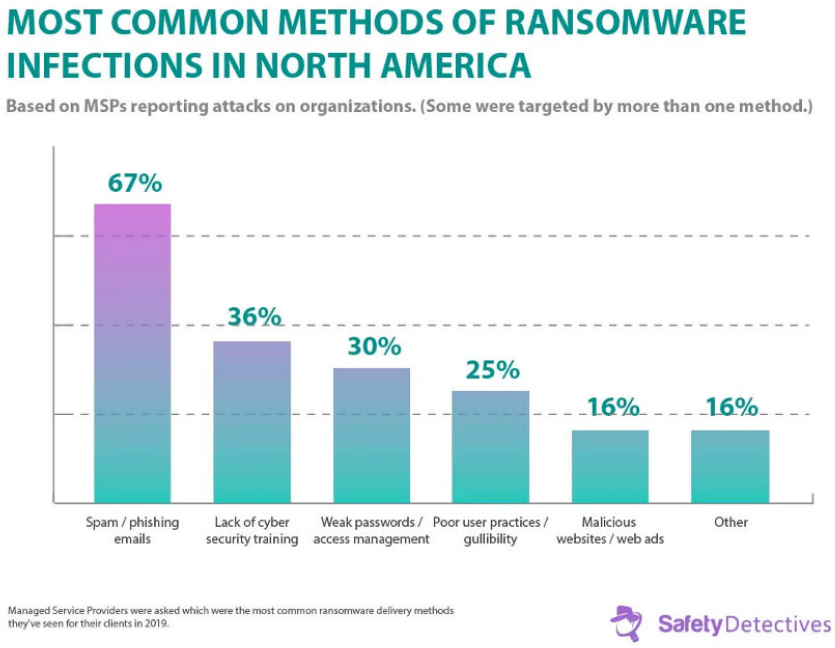

FIGURE 2

4. https://www.safetydetectives.com/blog/ransomware-statistics/
5. https://www.darkreading.com/vulnerabilities---threats/missing-patches-misconfiguration-top-technical-breach-causes/d/d-id/1337410

The Impact of Ransomware on Government Agencies and the Economy

The amounts of these ransom demands, as depicted in figure 3, have increased over time. As of first quarter 2020, they are averaging more than $100,000. In high-profile, high-impact events, such as the July 2020 hack of Garmin, the ransom demands are 100 times higher than the average.[6] Confidential sources have advised there are many more multiple million-dollar ransomware events than are reported in the mainstream media.

In addition, the number of companies getting hit with ransomware is also increasing dramatically. In August 2019, Malwarebytes[7] reported an almost constant increase in business detections of ransomware, rising a shocking 365 percent from Q2 2018 to Q2 2019.[8] It is likely this is reporting does not reflect the true increase due to many companies not disclosing that they were ransomed.

The true cost of an incident is much higher than the ransom paid. Companies suffer from significant downtime while responding to the incident and waiting for decryption keys. If the keys are even delivered by the criminals, there is often other damage to the IT environment and significant time and money must be expended to rebuild the network into an operational and secure state. Figure 4 shows the startling year-over-year increase in the downtime costs to victims.[9] Industry experts predict ransomware's startling growth will continue with total ransomware demands approaching $21 billion in 2021 (see figure 5).[10]

Europol advised that ransomware was the top cyber threat in 2019.[11] Ransomware is costing UK companies £346 million per year.[12] Three Australian companies were incapacitated following ransomware attacks in the first 6 months of 2020.

A health care organization was hit with a ransomware attack that affected all 1,500 of the organization's computers including its email server. The or-

FIGURE 3

6. https://www.forbes.com/sites/barrycollins/2020/07/25/will-garmin-pay-10m-ransom-to-end-two-day-outage/#37a595093164
7. https://www.malwarebytes.com/lp/sem/en/business.html
8. https://blog.malwarebytes.com/reports/2019/08/labs-quarterly-report-finds-ransomwares-gone-rampant-against-businesses/
9. https://www.safetydetectives.com/blog/ransomware-statistics/
10. Ibid.
11. https://www.voanews.com/silicon-valley-technology/european-union-finds-ransomware-top-cybercrime
12. https://www.acronis.com/en-us/articles/ransomware-attacks/

ganization's hospital began diverting patients from its emergency room as a result of the attack, slowing down response times, negatively impacting patient care, and putting lives at risk.

The Maze Ransomware gang breached and successfully encrypted the systems of VT San Antonio Aerospace, as well as stole and leaked unencrypted files from the company's compromised devices in April 2020. VT SAA is a subsidiary of ST Engineering, one of the largest firms listed on the Singapore Exchange and an engineering group with customers in the defense, government, and commercial segments in over 100 countries, and roughly 23,000 people across Asia, Europe, Middle East, and the United States.

During the attack, before deploying the ransomware payload to encrypt the company's servers, Maze claims to have stolen 1.5 TB worth of unencrypted files to be used as leverage to pressure the ST Engineering subsidiary into paying their ransom. As 'proof' that they breached VT SAA's network, Maze leaked over 100 documents consisting of financial spreadsheets, cyber insurance contracts, proposals, and expired NDAs. Maze first connected to one of VT SAA's servers via a remote desktop connection using a compromised Administrator account, then compromised the default Domain Administrator account and hit the company's domain controllers, intranet servers, and file servers on two domains. The memo also says that all the encrypted systems were fully recovered within three days after VT SAA's systems were encrypted by Maze Ransomware on March 7, 2020.

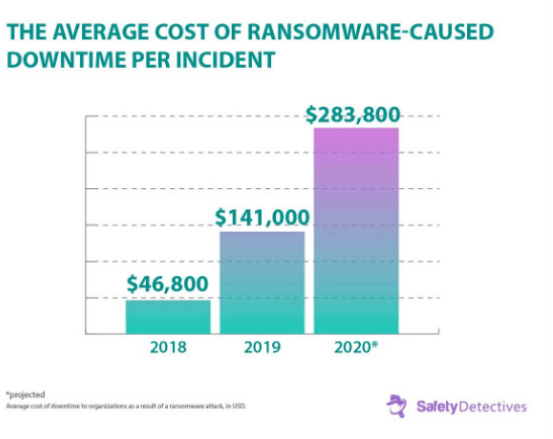

FIGURE 4

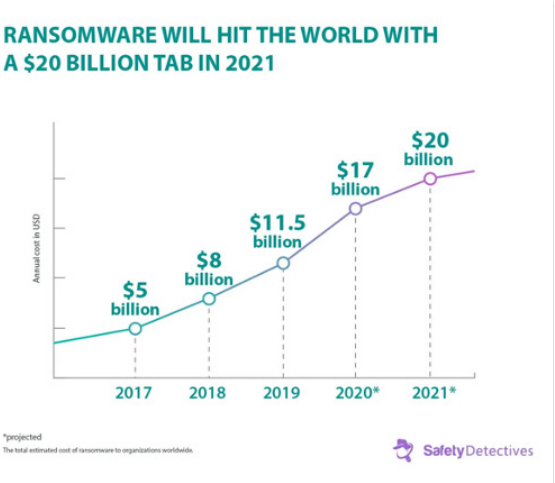

FIGURE 5

Key Statistics

The United States Federal Bureau of Investigation (FBI) estimates that there are 4,000 ransomware attacks every day, this equates to a ransomware attack every 40 seconds.[13] The following are key statistics regarding victims of ransomware attacks:

- 71 percent of ransomware attacks are targeted at small- to medium-sized businesses[14]
- Computer Weekly reports that 40 percent of spam now contains ransomware[15]
- Only four percent of organizations feel confident in their ability to stop ransomware[16]
- According to an IBM X-Force Ransomware report, 70 percent of businesses which were infected paid the ransom[17]
- Causing massive disruption, 63 percent of victims reported their systems were shut down for more than a day[18]
- Downtime costs US businesses $20 billion in revenue[19]
- Ransomware attacks have increased over 97 percent in the past two years[20]

Indirect Costs: Enforced Downtime and Reputation Loss

Business interruption costs are often five to ten times higher than direct costs. For small businesses, the average cost of ransomware related downtime in 2019 was $141,000, a more than 200 percent increase from $46,800 in 2018. This is 20 times higher than the average ransom request from small businesses ($5,900).[21]

Ransomware attacks are highly destructive and visible, leaving victims with no choice but to make it known to the public that they have been breached. Although the data can be restored, the public admission often yields in disapproval from customers, investors, and other stakeholders.

In conclusion, when assessing the potential risk emanating from ransomware attacks, businesses should factor in the payout, the downtime, damage to reputation, data loss, regulatory fines, contractual liability and more.

13. https://www.unitrends.com/solutions/ransomware-education
14. https://www.beazley.com/documents/2019/beazley-breach-briefing-2019.pdf
15. https://www.unitrends.com/solutions/ransomware-education
16. Ibid.
17. Ibid.
18. Ibid.
19. Ibid.
20. Ibid.
21. https://www.businesswire.com/news/home/20191016005043/en/Cost-Ransomware-Related-Downtime-Increased-200-Percent

The Growth of Ransomware Activity: RAAS and More Variants

Although early ransomware developers typically wrote their own encryption code when launching a ransomware attack, today's cyber criminals are becoming increasingly reliant on off-the-shelf ransomware libraries that are significantly harder to crack. This industry has become known as ransomware-as-a-service (RAAS).

Ransomware operators are franchising their software and processes. Criminals are able to purchase highly sophisticated ransomware from expert code writers in exchange for a percentage of the profits. One such RAAS is called Gandcrab. The criminal syndicate business model[22] is shown in Figure 6. This structure will dramatically increase the number of victims and the destructive effect ransomware will have on our economy.

Separately there are several ransomware variants which have been attacking critical infrastructure sectors in the United States: Ryuk (Fin6), Sodinokibi, Maze, Locker Goga, DoppelPaymer, Locky, Phobos, and Mega Cortex.

Predictions abound of increased ransomware attacks on a wide range of platforms:

- McAfee analysts suggest that individuals with a large number of connected devices and a high net worth are some of the most attractive targets.
- Attacks against Linux and Macs are expected to rise, according to IT Security Guru.
- Recent studies have shown that ransomware attacks are increasing more than 300 percent year over year.[23]
- Cybercriminals will target SaaS (Software-as-a-Service) and cloud computing businesses, which store and secure private data.[24]
- The Internet of Things (IoT) is primed to revolutionize life for businesses and consumers alike. However, the inherent vulnerability of this nascent technology can leave it wide open to ransomware attacks. A report by Kaspersky Lab[25] indicated that the number of IoT-focused malware attacks rose 10 X from 2016.

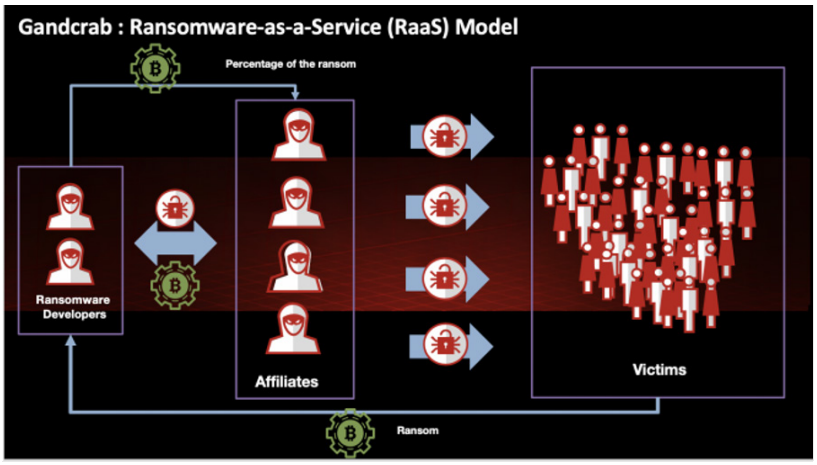

FIGURE 6

22. https://www.unitrends.com/solutions/ransomware-education
23. dimensiondata.com
24. Massachusetts Institute of Technology
25. https://www.kaspersky.com/about/press-releases/2018_new-iot-malware-grew-three-fold-in-h1-2018

Cryptocurrency and Money Laundering

Cryptocurrency and ransomware are closely intertwined, and many blame the rise of ransomware attacks over the past few years to the rise of cryptocurrencies. Cryptocurrencies are a vital part of the ransomware business model, as the majority of ransoms are paid in a form of cryptocurrency.

When criminals launder money via cryptocurrencies, they open online accounts with digital currency exchanges, which accept fiat currency from traditional bank accounts. They then cleanse the money by transferring money into cryptocurrency using mixers, tumblers, and chain hopping. Alternatively, they also use privacy coins, which are cryptocurrencies designed to be anonymous (Monero and Zcash). A Bitcoin tumbler or cryptocurrency tumbler is a service that mixes cryptocurrency tokens to obscure their origin.[26] They blur the origin and receipt of cryptocurrencies by mixing in a small number of cryptocurrencies with other cryptocurrencies, and then send smaller units of cryptocurrency to an address. Once the money's origin is properly obfuscated, the funds are then put into a legitimate financial system.

In August 2017, a group of researchers from Google, Chainalysis, University of California, San Diego and New York University analyzed ransoms paid in Bitcoin to determine how the ransom was laundered through the Bitcoin currency system.[27] Ninety-five percent of the ransoms were cashed out at a currency exchange in Russia.

In December 2019, the US Department of Justice indicted members of Evil Corp, a Russia-based hacking group, for operating a cyber-criminal organization which profited from numerous schemes including ransomware.[28] Without an extradition treaty with Russia, the investigative work yields no justice. According to Jody Westby, CEO of Global Cyber Risk, is quoted in an article about the investigation, "It is doubtful they will ever bring these two Russians to trial, because they remain in Russia, and it highlights… how hard it is to track and trace . . . cybercrime investigations."[29]

The Russian umbrella of protection facilitates additional attacks as seen in the recent Garmin ransomware event wherein the person behind the attack is alleged to be Maksim V Yakubets, a named leader in the December 2019 indictment described above.

26. https://blocksdecoded.com/what-is-bitcoin-tumbler/
27. https://elie.net/talk/tracking-desktop-ransomware-payments-end-to-end/
28. https://www.aljazeera.com/news/2019/12/russian-evil-corp-hackers-charged-100m-cyber-theft-191206054758063.html
29. https://altnewscoin.com/world-news/russian-evil-corp-hackers-charged-by-us-in-100m-cyber-theft/

The Regulatory Gap

The tracing of ransomware payments has revealed the criminal organizations are moving the cryptocurrencies through numerous wallets and other devices designed to conceal the ransom event as the source of the cryptocurrency. These wallets are either unaffiliated or strategically parked on exchanges around the world. In addition to the world governments regulating and enforcing AML upon cryptocurrencies, the international governments must work together to create standards and transparency as has been done for the global banking system.

Countries with cryptocurrency tax laws

- Argentina
- Austria
- Bulgaria
- Finland
- Iceland
- Israel
- Italy
- Norway
- Poland
- Romania
- Russia
- Slovakia
- South Africa
- Spain
- Sweden
- United Kingdom

Countries with cryptocurrency anti-money laundering and anti-terrorism financing laws

- Cayman Islands
- Costa Rica
- Czech Republic
- Estonia
- Gibraltar
- Hong Kong
- South Korea
- Isle of Man, Jersey
- Latvia
- Liechtenstein
- Luxembourg
- Singapore

Both

- Australia
- Canada
- Denmark
- Japan
- Switzerland[30]

30. https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf

These governments have enacted cryptocurrency regulations for various reasons. Some believe allowing cryptocurrency would ultimately result in the loss of economic power and shift towards decentralized economies. Many countries have banned cryptocurrencies as they deem them a threat to monetary policy. After Facebook introduced their Libra cryptocurrency project, there became growing concerns that cryptocurrencies might complicate the ability of central banks to control the money supply. For some governments, the regulation of cryptocurrency would add legitimacy to the industry, but for others, the regulation is not considered to be a pressing issue, especially considering the uncertainty among regulators on how to regulate the sector. A large-scale regulation could negatively affect the decentralization of cryptocurrency, but some regulation is necessary to legitimize the market. Regulations can protect a country's economy, their businesses, cryptocurrency traders, and reduce the risk of market manipulation.

In Europe, the overall perspective towards blockchain and cryptocurrencies have been positive, but recently, the European Union passed legislation to regulate it. Recently, the European Union signed its fifth Anti-Money Laundering Directive (5AMLD) into law. This law, as an effort to fight money laundering and terrorist activities, increases transparency around the owners of virtual currency by creating central databases comprised of crypto users' identities and custodian wallet addresses for Financial Intelligence Units (FIUs) to access. This law puts cryptocurrency under the same regulation as banks and other financial institutions, and any crypto service providers must register with financial authorities and identify and report any suspicious activity to FIUs.[31]

Cryptocurrencies are not legal tender in Canada, but the Canada Revenue Agency has created regulation to tax this security. Cryptocurrency exchanges are regulated and need to register with the Financial Transactions and Reports Analysis Centre of Canada (FinTRAC).

Japan was the first country to enact a law regulating cryptocurrency to protect customers of cryptocurrency exchanges and to combat money laundering and the financing of terrorism. Japan has the most progressive regulatory climate for cryptocurrencies and recognizes Bitcoin and other digital currencies as legal property under the Payment Services Act. Japan is the biggest market for Bitcoin and in December 2017, the National Tax Agency ruled that capital gains on cryptocurrencies are categorized as "miscellaneous income" and is taxed at a rate of 15–55 percent.

In the United States, the Bank Secrecy Act (BSA) rule [31 CFR 103.33(g)], often referred to as the "Travel Rule," requires cryptocurrency exchanges to verify their customers' identities, the identity of the original parties, and beneficiaries of transfers $3,000 or more and transmit that information to counterparties if they exist.[32] The travel rule was implemented by FinCEN in 1996 as part of anti-money laundering standards that applies to financial institutions in the United States.

The travel rule was first issued by FinCEN in 1996 as part of anti-money laundering standards that ap-

31. https://complyadvantage.com/blog/5mld-fifth-anti-money-laundering-directive/
32. https://www.sec.gov/about/offices/ocie/aml2007/fincen-advissCu7.pdf

plies to all U.S. financial institutions. FinCEN expanded the rule's coverage in March 2013 to apply to crypto exchanges as well, and in May 2020, the Treasury unit affirmed this. An inter-governmental global organization devoted to battling money laundering and terrorism financing, Treasury led-Financial Action Task Force (FATF), likewise directed crypto exchanges and regulators around the world to comply with the travel rule, giving them about a year to do it with the clock starting in June 2020.

In March 2013, FinCEN published FIN-2013-G001, Guidance on the Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual currencies. FinCEN confirmed recognition of virtual currency exchanges as it falls under the moneyservices business classification. This meant that any entity conducting business as a virtual currency exchange should immediately register with FinCEN and ramp up efforts to create a sound anti-money laundering compliance program.

This position was further evidenced two years later with the first enforcement action against a virtual currency exchange when FinCEN and the U.S. Attorney's Office for the Northern District of California (USAO-NDCA) gave Ripple Labs, Inc. a $700,000 civil monetary penalty for its disregard to report suspicious activity and implement an effective anti-money laundering program. To avoid a criminal investigation, Ripple Labs, Inc. signed a settlement agreement with the USAO-NDCA. Ripple bounced back a year later and was awarded the second Bit License by the NYDFS.

Despite the Travel Rule and efforts to increase enforcement, calls to increase regulation of the cryptocurrency market continue. In a paper published in March 2019 by the Brookings Institute,[33] Timothy G. Massad, Senior Fellow, The John F. Kennedy School of Government, Harvard University called for increased regulation ahead of a significant cyber-attack or fraud. Although this paper is directed to the United States, it presents sound recommendations that must be implemented internationally in order to best reduce the risk of cryptocurrencies being used, as it is today, to deliver proceeds of criminal activities back to cyber criminals.

In October 2020, the U.S. Treasury issued an advisory warning U.S.-based businesses they might be in violation of OFAC regulations if they were to make ransomware payments to malicious cyber actors. We see the OFAC advisory as putting additional burden on the victims of ransomware by potentially eliminating the ability to obtain decryption keys. The OFAC sanctions enforcement only hurts the victims of ransomware and is not the way we recommend moving forward.

33. https://www.brookings.edu/wp-content/uploads/2019/03/Economis-Studies-Timothy-Massad-Cryptocurrency-Paper.pdf

Conclusion

Ransomware is the equivalent of a criminal organization's tax on business. The global banking industry made great strides in degrading global drug cartels and identifying their members by creating anti-money laundering rules for financial institutions. Similarly, we must attack the business model of ransomware operators.

Anti-money laundering laws have been effective when compliant financial institutions adhere to the requirement to "know your customer." The global cryptocurrency eco-system does not require nor universally apply this principle. Only a limited number of cryptocurrencies and exchanges are conducting business in the spirit of legitimacy and with the intent to root out the use of cryptocurrencies to facilitate criminal behaviors.

Regardless of the level of anonymity afforded by cryptocurrencies, criminals must exchange their cryptocurrency for fiat money (currency issued by a government) in order to make it a fungible asset. The monitoring of cryptocurrencies via public ledgers and blockchain analytics has led to the identification of the points at which the ransomware proceeds were converted back to traditional currency.

A blockchain-based platform gives regulators, auditors, and other stakeholders an effective and powerful set of tools to monitor complex transactions and record the audit trail of suspicious transactions across multiple wallets. Since all the information is stored in the blockchain and available in each node, suspicious activity can be detected. However, regulators and law enforcement are not monitoring this activity in real time. Nor do the current investigative methods have any impact when an indicted mastermind sits behind the veil of a border while he executes ransomware attacks causing global businesses to lose millions.

Various methods can be implemented to contrast money laundering involving cryptocurrencies:

- AML procedures can be strengthened at financial institutions;
- transaction monitoring can be continuous and contemporaneous, followed by swift execution of legal process to inhibit or disrupt the money laundering process;
- regulations can be improved;
- cryptocurrency exchanges can be regulated, especially advanced digital exchanges and exchanges offering to purchase primary cryptocurrencies;
- fines can be levied when you "know your customer" requirements are not adhered to by cryptocurrencies.

Regulations increase operating costs for cryptocurrencies. This may lower the trading values of cryptocurrencies in the short term. However, in the long term, it is expected that regulation would stabilize the cryptocurrency market and lessen the use of cryptocurrencies by cyber criminals.

Greater AML regulation and enforcement in the cryptocurrency eco-system would degrade and disrupt the ability of ransomware operators to conduct anonymous ransomware operations.

International governments must set the standard for responsible cryptocurrency markets and work collaboratively to create standards in global cryptocurrency markets which reduce the ability of criminal organizations to use cryptocurrencies to profit from the ransom of legitimate businesses.