Service/Utility Token: BITCQR (BCQR)

Ethereum (ERC20 Compliant Token)

Jose A. Neto

Former DoD INFOSEC Special Agent

Doctoral Candidate - DIT (Cyber Security)

Abstract

With over a half trillion dollar in market capitalization, the digital market represents an emergent alternative global financial ecosystem. In parallel, the cost of cybersecurity spending in 2017 represented $86.4 billion according to Gartner, and it is expected to exceed $1 trillion in over five years. The BITCQR token will provide the secure configuration management solution to strengthen the cybersecurity posture of individual consumer & enterprise computing systems. We are the premier cybersecurity solutions provider with the goal to secure and safeguard this half a trillion dollar industry. The world-class cyber team at BitCQR is leveraging years of knowledge and experience in securing and protecting highly sensitive military and government environments and making cybersecurity accessible to consumers and small businesses around the world. We believe everybody is entitled to protect their digital lives with the highest military-grade cybersecurity.

Table of Contents

Introduction

In 2017, the awareness of Bitcoin and other digital assets reached new heights around the world. With over a half trillion dollar market capitalization, the digital market represents an alternative global financial technological (FINTECH) ecosystem. In parallel, the cost of cybersecurity spending in 2017 represented $86.4 billion according to a Gartner study and is expected to exceed $1 trillion in over five years as shown in Figure 1. Cyber attacks have impacted individuals, small businesses and large enterprises resulting in both financial losses as well as negative social branding reputation.

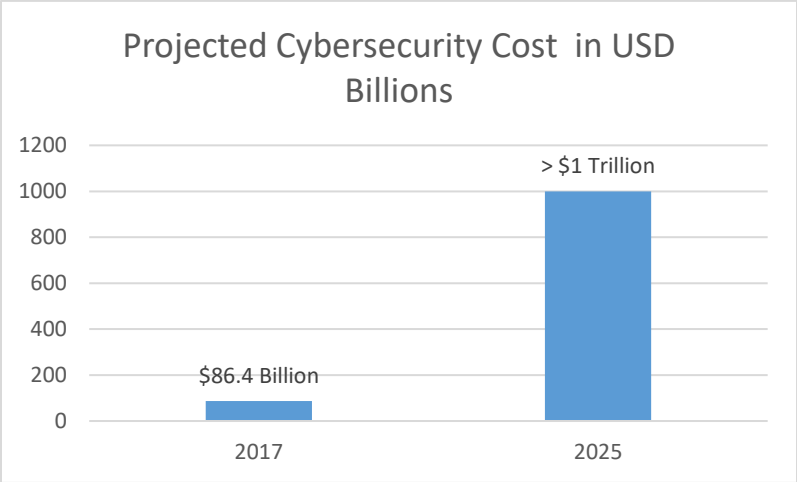
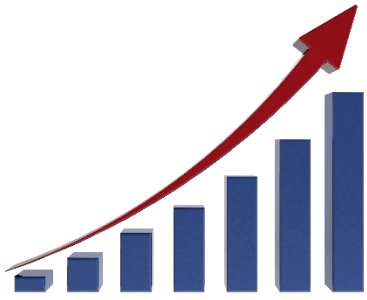


Figure 1. Projected cost of Cybersecurity

At a very alarming rate, it is projected that 6 billion people will be impacted by cyber criminals by 2022. Consequently, in the corporate world, Ginni Rometty, IBM's president and CEO, said, "Cybercrime is the greatest threat to every company in the world." (Morgan, 2017.)



In the federal space, the Federal Bureau of Investigations stated "Cyber intrusions are becoming more commonplace, more dangerous, and more sophisticated. The threat is incredibly serious and growing." (Cyber Crime, 2017).

In 2015, under the leadership of former president Barack Obama, the executive branch in coordination with Congress passed the Cybersecurity Act of 2015, with the goal to provide the necessary tools to strengthen our nation's cybersecurity.

Another enacted cybersecurity initiative was the Cybersecurity National Action Plan (CNAP), focused on raising cybersecurity awareness and empowering Americans to take better control of their digital security. The White House stated that cybercriminals have come to the realization that online attacks are often easier than conducting an attack in person. Former President Obama contended that "if we are going to be connected, we also need to be protected."

The BITCQR security solution powered by the (BCQR) token will provide the secure configuration management services and consulting needed to strengthen the cybersecurity posture of individual or enterprise computing systems. The traditional security tools used to protect a computer system such as anti-virus software are useful in detecting known malware but do not strengthen the core cybersecurity posture of the operating system. Integrated or external network firewalls also provide additional port filtering mechanisms for communication sockets

but do not address the hundreds of settings within an operating system that can be exploited if not properly configured.

The most important step in establishing military—grade cybersecurity in systems is starting with a system baseline with the most restrictive environment offering the highest protection while still maintaining the needed functionality.

Decentralization & Blockchain Technology

The most significant feature of blockchain technology is the concept of decentralization. Through these decentralized peer-to-peer wallet solutions, individuals are able to process transactions without the need of a third-party all based on high-integrity cryptographic transactions. The deployment of this revolutionary FINTECH solution not only facilitates the control of digital value globally, but it also forces the public to become a personal digital bank with the responsibility to safeguard their cryptographic assets and value.

With the proliferation of different types of online malware, consumers are vulnerable to viruses, worms, Trojan horses, rootkits and other types of malware that can not only cripple their functionality but compromise the private information such as Bitcoin or Alt-Coin private keys.

The importance and need for cybersecurity in our lives

What is Cybersecurity?

According to Amoroso (2006), “cybersecurity involves reducing the risk of malicious attack to software, computers, and networks. This includes tools used to detect break-ins, stop viruses, block malicious access, enforce authentication and enable encrypted communications. The technological landscape has radically changed within the past three decades. The need for

authentication, encryption, and secure environments is no longer a commodity but a necessity in our daily operations.

Cybersecurity awareness and education

Our mission and commitment to our global cybersecurity community of BitCQR users and commercial clients begin with cybersecurity awareness and education. Proctor (2016) contend that users are the primary targets of data breaches for they are perceived as the weakest link in the system. A plausible countermeasure and mitigation against this type of social cyberattacks can be implemented through cybersecurity training programs and security presentations to non-technical users. In the past, our BitCQR team members have briefed government and military audiences as well as presented in industrial security conferences such as the Florida Industrial Security Working Group (FISWG). These events have helped educate the public and local businesses in raising awareness of the important role of cybersecurity. Our global education and awareness campaigns will consist of producing short cybersecurity training videos that will be disseminated through all our social media platforms for the benefit of all our global BitCQR community. We firmly believe, that this social initiative will also establish the BitCQR brand as a leading entity providing the highest level of cybersecurity in our emerging FINTECH and commercial markets and will drive the demand of our services and exposure of our ERC20 (BCQR) token offering.

Cybercriminals and their motives

The relative anonymity that the internet provides has increased the number of perpetrators involved in online hacking in comparison to the traditional crime scene (Longe et al., 2010.) The most significant challenge encountered by law enforcement entities has been the proximity of the crime location and the criminal's location. Wada et al. (2012) contend that

physical constraints and security measures are perhaps the only deterrents that can slow down or mitigate an attack. Although there is no such thing as perfect cybersecurity, our objective is to diminish the exposure to cyber threats and mitigate risk by keeping our global cyber community informed of the latest exploits and malware used by cybercriminals.

The need for cybersecurity in protecting intellectual property and sensitive personal or patient information

It is projected that Cybercriminals will broaden their efforts and target smaller companies as a bridge to target the larger business entities, due to their lower cybersecurity posture and accessibility and partnership with other vendors (Greenwald, 2015.) In the healthcare industry, Ponemon (2016) reported that nearly 90 percent of healthcare organizations included in their research study had experienced a data breach, costing the healthcare industry over $6.2 billion in damages and corrective actions. Among the top three type of cyber attacks are ransomware, malware, and denial of service.

Effectiveness of our BitCQR Secure Configuration Management Solution

Our experts have confirmed that a typical brand new Widows computing system, possesses an average military cybersecurity posture of 39% as shown in figure 2. After configuring a system to military-grade specifications, our locked down systems yielded a 97% cybersecurity posture as shown in figure 3, while still maintaining all the functionality needed for day to day operations. This level of military-grade protection is an active requirement for federal contractors to maintain cybersecurity compliance.

There is also a misconception that Windows systems are the only vulnerable computing systems, but the reality is that all operating systems have vulnerabilities and attack vectors. This can be demonstrated by the famous Shellshock Bash Bug that affected Linux and OSX systems a while back. This vulnerability allowed remote execution of the vulnerable systems that could potentially compromise private information, delete files, and activate system resources such as webcams (Andrade, 2016). We dedicated the initial development of our secure configuration management utility for the Windows Operating system (OS) because it is the most widespread OS. During 2018, we will develop other security configuration management tools for Linux based systems and Apple's OSX.

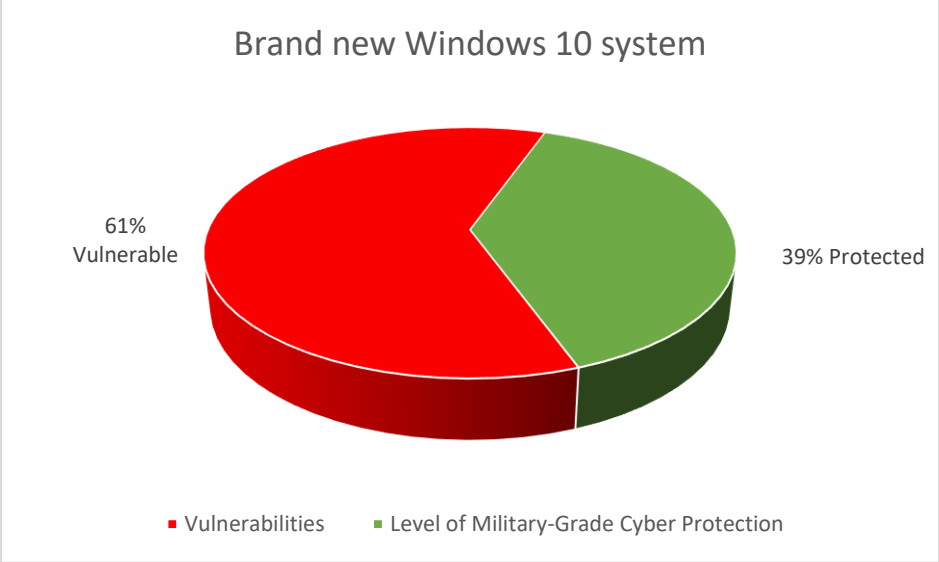


Figure 2. Brand New Windows System

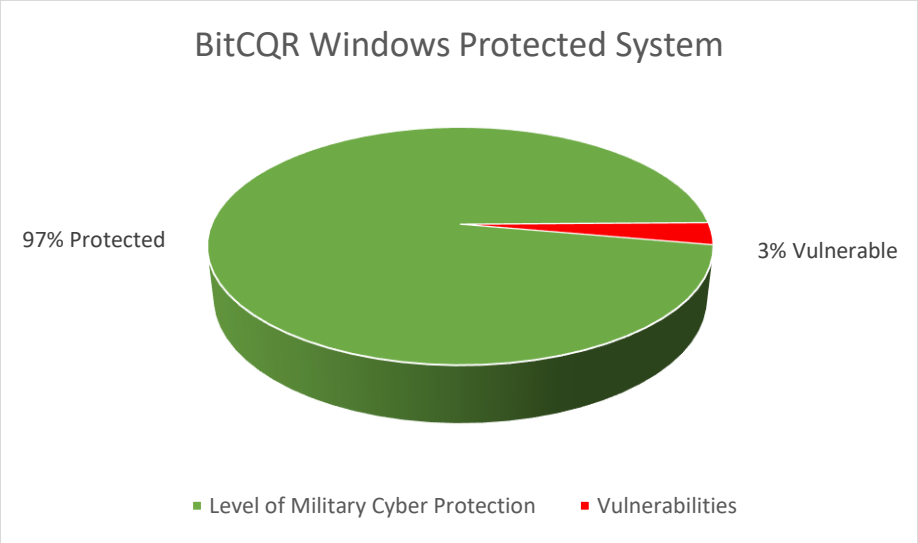


Figure 3. BitCQR Protected system

BitCQR Services

Our Comprehensive/Holistic approach to Cybersecurity Defense encompasses the following layers of protection.

Configuration Management/System hardening

The first layer of protection begins with having a personal or business computing platform configured with the highest level of protection. Our system hardening processes implement military-grade cybersecurity baselines and techniques to strengthen your system and minimize exposure through our BitCQR configuration management solution.

Vulnerability Assessments

Vulnerability Assessments represents the initial step in information gathering to reveal the current cybersecurity posture of a system an organization. This process will assess all connected computing nodes in addition to all network peripheral and devices. The resulting vulnerability assessment report will identify any discovered vulnerabilities and potential attack vectors that can be compromised. The scope of this evaluation includes operating systems, third-party applications and vendor firmware updates among other published vulnerabilities.

Penetration Simulation/Testing

Penetration Simulation/Testing builds upon the initial vulnerability assessment, and simulates the exploitation of the discovered attack vectors to provide a more detailed report of the severity of exploits. This offensive intelligence approach may momentarily disrupt daily

operations to measure the impact of possible attacks and provide the organization with a realistic impact analysis of their systems. The additional testing of the discovered vulnerabilities, eliminates false/positives and delivers a more concise and detailed report of eminent threats.

Incident Response Management

Due to the lack of cybersecurity awareness, some of our clients make an initial contact with us after they have been compromised. During this stage, there are many critical steps that must be considered. First, how soon can the organization recover to normal working conditions? Evidence must also be preserved through proper chain-of-custody procedures to preserve its forensic integrity for legal proceedings. The attack vector used must be analyzed to prevent future repeated exploits through a careful analysis of injected malware or malicious scripts.

Information Security Training

Behind every cyberattack, there is always a human element and motive. We provide a range of cybersecurity training content for end-users, system administrators and executive leadership within an organization or entity.

- Basic Cybersecurity Awareness training
- Technical Best-Practices on maintaining a secure IT Infrastructure
- Executive Cybersecurity Top-Down leadership planning

Government Compliance Consulting

With the emergence of FINTECH solutions and the evolving legal landscape of government compliance by organizations such as the Securities Exchange Commissions (SEC),

Financial Crimes Enforcement Network (FinCEN), Financial Industry Regulatory Authority (FINRA) and Commodity Futures Trading Commission (CFTC), our compliance experts will assist you in meeting the expected government compliance baselines.

Continuous Monitoring Protection

Given the increase on Advanced Persistent Threats (APT) in cyber space, experts concur that continuous monitoring and protection is needed to minimize the risk of exploitation. BitCQR is prepared to create and design a custom security continuous monitoring plan for your organization.

Physical Security Taskforce for High-Profile Individuals

As digital value becomes more and more relevant in our society, High-Profile individuals in the digital market have become targets for organized cybercrime. Our BitCQR physical security taskforce is comprised of former Marines, SAS and MI6 trained personnel. Your physical security will be handled and managed by an elite group of BitCQR Protective Agents.

The BITCQR Utility token

The purpose of the BITCQR token is to provide a global mechanism for the payment of the cybersecurity services. These funds will be used to pay developers, security researchers, and on-going operations to serve worldwide customers and partners. As compliance cybersecurity experts, we will also establish a framework to assess the cybersecurity posture of digital exchanges, with the goal to ensure these FINTECH entities effectively protect their technical environments in the interest of their customers. Through this digital token offering, we are decentralizing the cost of cybersecurity within all our global clients and participants, significantly reducing the cost of our services by spreading the cost of operations throughout our global community. Through this global cyber initiative, we are able to make our military-grade cybersecurity services affordable to the consumer audience as this has been inaccessible in the past due to high costs. Small businesses will also have access to better cybersecurity protection and awareness, without an exuberant cybersecurity budget.

We are BITCQR, the future of global Cybersecurity for the consumer and FINTECH industry.

https://etherscan.io/token/0x3e924b6ae9f6854a94a57ff89985716cd11267d3

Disclaimer

Please make sure to read this notice before proceeding. The information presented on this whitepaper and/or any of the documents available on the BITCQR.io website is by no means an invitation or offer to any person to purchase securities or shares in any company, including but not limited to the BITCQR (the "Company"). The information is presented for information purposes only and may not contain all of the relevant information regarding the purchase of BITCQR Utility Tokens ("Token"). As such the information does not necessitate the taking of any action by the readers of this document or by the shareholders of the Company. The shares of the Company are not being presently offered for sale or subscription in any jurisdiction.

Readers of this document will not be considered investors and/or clients of BITCQR just by virtue of access to the bitcqr.io website or reading this document. Readers of this document and visitors of the www.bitcqr.io website should not construe discussion or information contained herein as personalized advice.

The BITCQR founders, team, shareholders, advisors, partners or affiliates shall not be liable for any errors or inaccuracies, regardless of cause, nor will they be liable for and delay or interruption in the project roadmap. The Tokens referred to below have not been registered by the US Securities and Exchange Commission, nor have they been registered with any other authority in any jurisdiction. purchasers participating in the token sale should be aware of the risks involved.

BITCQR is not an investment advisor, a banking institution, a broker or a dealer. BITCQR does not participate in the offer, sale, or distribution of securities. BITCQR does not provide any investment advice. None of the information published or presented on this document or on the

bitcqr.io website constitutes a solicitation, an offer, or a recommendation to buy or sell any financial instrument or to effect any transaction.

The Company does its best to present the most accurate information. Under no circumstances can or do the owners, authors, contributors, and/or partners warrant the accuracy, completeness or usefulness of the content found on the bitcqr.io website and/or any of the documents available on it, including this one, for any particular purpose.

Under no circumstances can or do the owners, authors, contributors, and partners make any promises or warranties, nor accept responsibility for any liability, injury or damage that you may incur or cause. BITCQR makes no promises that our service will be delivered on schedule, and error free. Therefore all of the content and information provided on this document and/or the bitcqr.io website should be taken on an "as is" basis. Decisions based on information contained on the bitcqr.io website and/or this whitepaper are the sole responsibility of the person viewing the website or reading this document.

In exchange for utilizing the information on the website and/or whitepaper, the visitor agrees to indemnify and hold fund its officers, directors, employees, affiliates, agents, licensors and suppliers harmless against any and all claims, losses, liability, costs and expenses (including but not limited to attorneys' fees) arising from the use of the website and/or whitepaper, or from any decisions that the viewer makes based on such information.

Prospective buyers should read in detail the BITCQR white paper, smart contract and other relevant documents and seek independent legal and financial advice, or independently research and verify any information that they find on the bitcqr.io website or in the linked documents.

The website and/or any document featured on it do not contain any legal or financial advice and potential purchasers should refer to the applicable provisions of the securities legislation in their respective jurisdiction for the purpose of the investment or consult with a legal and financial advisor.

Tokens are being offered only in those jurisdictions where they may be lawfully permitted to be offered for sale and therein only to those persons to whom they may be lawfully offered for sale. Prospective buyers should inform themselves as to the legal requirements and tax consequences within the countries of their citizenship, residence, domicile, and place of business with respect to the acquisition, holding, or disposal of Tokens, and any foreign exchange restrictions that may be relevant, and keep in mind that the offer and sale of Tokens in certain jurisdictions may be restricted by law. This offer by BITCQR does not constitute an offer to sell or the solicitation of an offer to buy in any country, state or jurisdiction to any person to whom it is unlawful to make such an offer or solicitation in such country, state or jurisdiction, especially in China, South Korea, Macau, Russia and Dubai.

The offering by BITCQR of BITCQR Utility Tokens have not been and will not be registered under the United States Securities Act of 1933, or any European union or United States state Blue Sky securities laws or the Singapore securities laws or the securities laws of Cayman islands or the laws of any other jurisdiction. The interests will be offered and sold under exemptions under the laws of the jurisdictions where the offering will be made. Consequently, purchasers will not be afforded the protections of those laws.

References

Cyber Crime. (2017, March 22). Retrieved February 10, 2018, from https://www.fbi.gov/investigate/cyber

Kaplan, J. M., & ProQuest Ebooks. (2015). Beyond cybersecurity: Protecting your digital business (1st ed.). Hoboken, New Jersey: John Wiley & Sons, Inc.

Morgan, S. (2017, July 26). Is cybercrime the greatest threat to every company in the world? Retrieved February 10, 2018, from https://www.csoonline.com/article/3210912/security/is-cybercrime-the-greatest-threat-to-every-company-in-the-world.html

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review, 4(10), 13-21. Retrieved from http://library.capella.edu/login?qurl=https%3A%2F%2Fsearch.proquest.com%2Fdocview%2F1638205509%3Facco

Amoroso, E. 2006. Cyber Security. New Jersey: Silicon Press.

Kim, L. (2018). Cybersecurity matters. Nursing Management (Springhouse), 49(2), 16-22. 10.1097/01.NUMA.0000529921.97762.be

Proctor, W. R. (2016). Investigating the efficacy of cybersecurity awareness training programs

Andrade, J. (2016, July 14). What is the Shellshock Bash bug and why does it matter? Retrieved February 20, 2018, from https://www.engadget.com/2014/09/25/what-is-the-shellshock/

Longe, O., Osofisan, A., Kvasny, L., Jones, C. and Nchise, A. (2010). "Towards A Real-Time Response (RTR) Model for Policing the Cyberspace", Information Technology in

Developing Countries, Vol. 20, No. 3. http://www.iimahd.ernet.in/egov/ifip/oct2010/olumide-longe.htm

Wada, F., Longe, O., & Danquah, P. (2012). action speaks louder than words - understanding cyber criminal behavior using criminological theories. Journal of Internet Banking and Commerce, 17(1), 1.

Greenwald, J. (2015). Cyber criminals widen scope of industries to attack. Business Insurance, 49(11), 19. Retrieved from http://library.capella.edu/login?qurl=https%3A%2F%2Fsearch.proquest.com%2Fdocview%2F1683622590%3Faccou

Ponemom, L. (2016). News & Updates. Retrieved February 20, 2018, from https://www.ponemon.org/blog/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data