Today's trust-based solutions may become non-viable in the future. As use of the cloud grows, we are experiencing a shift in resource allocation from on-premise to off-premise systems. As systems move to cloud hosted environments, the loss of control over the access network becomes a concern. We need to figure out a solution, a possible solution is a cyber trust score

Earning Trust in the 21st Century

Cloud Security Alliance - DC (CSA-DC) Research

Author: Sakraney, Simran [USA]
CSA-DC Research Chair: Dr. Spina, Mari [USA]

CSADC Washington DC Chapter cloud security alliance®

Table of Contents

1.0 Background

In today's interconnected and technology reliant world, the expectation of trust and need to trust is growing. Today's trust-based solutions may become non-viable in the future. As use of the cloud grows, we are experiencing a shift in resource allocation from on-premise to off-premise systems. As systems move to cloud hosted environments, the loss of control over the access network becomes a concern. Today's trust-based solutions typically start at the network level. If a user has access to a network, they are typically trusted to have access to some or all of the resources, data, and systems on that network.

But, when networks are unknown and untrusted, how is trust acquired? Zero Trust (ZT) architectures seek to provide access control techniques that assume the network is not trustworthy. One of the approaches suggested by industry is the use of trust scores. Like a credit score, a cyber trust score could be used to assess the risk potential associated with allowing any given user access to systems and information. But how would a trust score be calculated? Current approaches smack of a violation of privacy where the right to gain access is issued only by agreeing to be monitored.

This paper addresses the technical, social, policy, and regulatory issues associated with creating trust frameworks in a Zero Trust world. Industry and government are called to solve issues in ways that continue to protect the right to a users' privacy.

Traditional Domain Based Trust Systems

Transitive Trust is a two-way relationship automatically created between two domains in a forest. For example, transitive trust may allow the resource domain to trust the account domain through a chain of trust relationships, even between intermediate domains [16]. Inter-Domain Trust occurs when a domain provides another trusting domain with its users' security access token. The trusting domain may use the token to determine if the user has the necessary permissions to allow access to its' resources. In operation for example, a user logs into the first trusted domain and then opens a file in the other trusting domain without having specifically logged into the other domain [16].

Authentication is the process of an entity proving its identity to another entity, often a system that the entity is attempting to access [15]. Authentication can take place between any system, such as a computer program and an end user (human), a computer system, a piece of hardware, or mobile device. Credentials are used to authenticate a user. Credentials are considered proof of identity. There are different types of credentials; for example, Public Key Infrastructure (PKI) that use digital certificates, passwords, pins, even biometrics such as fingerprints and iris scans [15].

Trust today is achieved between networks and domains using Single Sign On (SSO), Federation, and Kerberos. SSO is a session and user authentication service that permits an end user to enter one set of login credentials (such as a name and password) to access multiple applications. SSO allows for a user's identity to provide access across multiple service providers [15].

Federated Identity Management (FIM) is an arrangement that can be made between multiple enterprises to let subscribers use the same identification data to obtain access to the networks of all the enterprises in the group. Federation works by establishing common standards and protocols to manage and map user identities between Identity Providers (IdPs) across organizations (and security domains) [15]. When two domains are federated, a user can authenticate to one domain and then access resources in the other domain without having to perform a separate login process due to trust relationships previously established via digital signatures, encryption, and PKI. In order for FIM to work efficiently, the partners must have a sense of mutual trust [15].

Identity and access management (IAM) is a framework of business processes, policies and technologies that enables digital identities to be managed. Federated Identity Management is a sub-discipline of IAM. Federation allows SSO to occur without requiring passwords because the federation server knows the username for a person in each application and presents that application with a token via SAML, OpenID, WS-Trust, WS-Federation and OAuth [15] The token implies that, "this person is an accepted user of domain\johndoe or johndoe@example.com". As a result, no password is required for the user to login to each system [4].

Kerberos is a prominent example of a trusted SSO systems and works as a computer-network authentication protocol [15]. Kerberos uses tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Kerberos has the foundation of symmetric key cryptography and requires a trusted third party. For certain phases of authentication, Kerberos may use public-key cryptography [15].

Zero Trust Obviates the Network

When technology advanced to the point where individuals could access data wherever they are through an app via cloud computing, the game changed because the perimeter itself lost form and function. Traditional domain-based network security is becoming obsolete with the migration to cloud services and the surge to bring your own device (BYOD). The Zero-Trust model was developed as a response to the realization that the domain-based perimeter security approach is no longer sufficient given hackers have found ways through corporate firewalls [15][16].

As a solution, technologists began using Zero Trust Architecture (ZTA), as defined by the National Institute of Standards and Technology, provides a collection of concepts, ideas, and component relationships (architectures) designed to eliminate the uncertainty in enforcing accurate access

decisions in information systems and services. [22] In fact, every actor, system, or service shall be thoroughly verified. The Zero Trust model conducts more due diligence than perimeter-based security did in the past. Zero Trust allows enterprises to define internal trust boundaries to granularly control traffic flow, enable secure network access, and implement network monitoring. Access decisions are made based on user locations and associated data used to determine whether or not a user, machine or application is trustworthy enough to be granted access to a particular segment of the enterprise. Zero Trust establishes trust zones where resources that have the same trust level and function will operate alongside one another. This, in turn, minimizes pathways and malicious threats. Zero Trust encourages the maximum security and controls to be implemented for the highest level of network visibility, threat detection, and compliance reporting. Zero Trust solutions may include multi-factor authentication, strong encryption, file system permissions and the enabling of analytics for threat detection and prevention. Zero Trust also supports the concept of least privilege [16].

But Zero Trust Architectures (ZTA) of today may not be sufficient to make trust determinations. When introduced, Google's Beyond Corp. proposed the trust or inference engine. Such a system needs appropriate information from which to make trust assessments. [14]. Trust scoring approaches have been posited. But what measure should be used and how will such measures impact use and utility of systems?

2.0 Solution Landscape

Trust Scoring Models for Entities

FICO® created an Enterprise Risk Suite, a pilot program that allows businesses to access their FICO® Enterprise Security Score. The score is derived from machine learning models that forecast the likelihood of a future breach event by analyzing key risk indicators including the health and hygiene of IT systems, network infrastructure and software and services. These current and historical data signal behaviors are compared to past behaviors of organizations that have, and have not, suffered a material data breach. This worldwide program gives any company the ability to assess their cyber security posture before they are assessed by other organizations in their supply chain free of charge [19].

Other vendors are attempting to create enterprise cyber trust scores as well. RiskSense, a vulnerability management firm, offers a service that scans agency assets, applications, databases and networks for vulnerabilities and assigns a cybersecurity risk score, much like a credit score [18] According to Anand Paturi, VP of Risk Sense, the “Risk Sense-RS3" score is essentially a prediction of the level of peril the organization is subject to, based on its vulnerabilities and all the contextual data [18]. The results have been positive because everyone is familiar with the financial credit score system. All agencies in Arizona currently have scores of 700, and Risk Sense is trying to bring them all to 725. These scores help prioritize patching, but they also give the

state's security experts an easier way to communicate a system's security posture with leadership and those with whom they collaborate [18].

Sift is another Digital Trust Platform (DTP) which is powered by Live Machine Learning and claims to automatically and dynamically enhance digital interactions in real time based on individual risk scores that are developed by predicting a users' intent in real time [2]. Sift protects businesses from all vectors of fraud and abuse including payment fraud, account takeover, fake accounts, and abusive user-generated content. According to the VP of Sift, Geoff Huang "The objective of Sift is to make the best predictions of outcomes for behaviors on the internet." [8]. Sift allows for the overall trustworthiness of online users to be determined accurately and in real time which allows for businesses to be able to enter new markets that were previously inaccessible due to security concerns. Companies who use Sift can give trusted users a positive digital experience that allows them to build highly valuable long-term trusting relationships. Many global brands such as Twitter, AirBnB, Yelp, Indeed, Zillow and Wayfair use Sift [2]. Sift allows validated businesses to publicly display a badge promoting that they take trust and safety seriously and protect users through the adoption of advanced technology and industry insight. This program strengthens the digital trust network by connecting users with trustworthy businesses which creates a win-win situation. According to an article in the Wall Street Journal, more than 16,000 signals are used to inform the "Sift score, which is a rating that ranges from 1 to 100" [11]. The Sift score is used to flag devices, credit cards and accounts owned by any entity whether it be a human or robot that a company may want to block. This score is like a credit score, but for overall trustworthiness, says a company spokeswoman [11]. There is no way to find out your Sift score. Companies use products like Sift and Secure Auth to detect bots and decipher who to subject to additional screening, which for example, would entail requesting the user to upload a form of ID [2].

The cyber risk score for companies is often based on industry, cyber supply chain, vulnerabilities, network connectivity, interaction efforts, etc. [6]. Insurance companies use a scoring system to provide an empirical foundation for issuing policies and pricing insurance premiums which is known as actuarial tables. It gives high risk companies a clear benchmark and incentive to purchase insurance and prioritize internal investments to mitigate specific cyber risk areas. Many of these scores are curated by machine learning models which we know are not yet perfect and have issues of their own. Many of the security rating companies use a combination of data points collected or purchased from public and private sources and proprietary algorithms to articulate an organization's security effectiveness into a quantifiable measure or score. As these ratings rely in part upon the quality and breadth of the data they use, the variety of sources and the dynamic nature of the environment create risks of producing ratings that can potentially be inaccurate, biased, irrelevant or incomplete.

Trust Scoring for Individuals

In 2014, Beijing established a Plan for Establishing a Social Credit System as a nationwide, regulated project. In 2015, the Central Bank of China granted license to 12 pilot projects including China's biggest tech giant, Alibaba which released Sesame Credit. By 2016, in addition to Sesame credit, 31 pilot projects were established including Social Credit Numbers, The Honest Shanghai app and Tencent credit [21]. The apps are currently voluntary and give users a public credit score based upon the social, financial, personal and behavioral habits of citizens. The intention of these apps is to judge the trustworthiness of the citizens and encourage them to be more honest. The apps are currently a part of a pilot program and track a citizen's credit history, financial purchases, as well as their behavior towards friends and family which is inputted into an algorithm and calculated to create a score [21]. An individual's score moves up or down based on positive or negative actions. Depending on an individual score, one may end up on a black list or a red list, Beijing's version of a white list. Both lists are readily available on a website called China Credit.

In China, the exact methodology of how the score comes to be, is a secret just as in America the exact breakdown of the financial credit score is also not readily available [10]. It is important to note that this also may be due to censorship and general lack of transparency in Beijing. Author of the book "Who Can You Trust? How Technology Brought Us Together – and Why It Could Drive Us Apart" Rachel Botsman gathered information from Chinese and Western media sources which has been summarized in the diagram below.

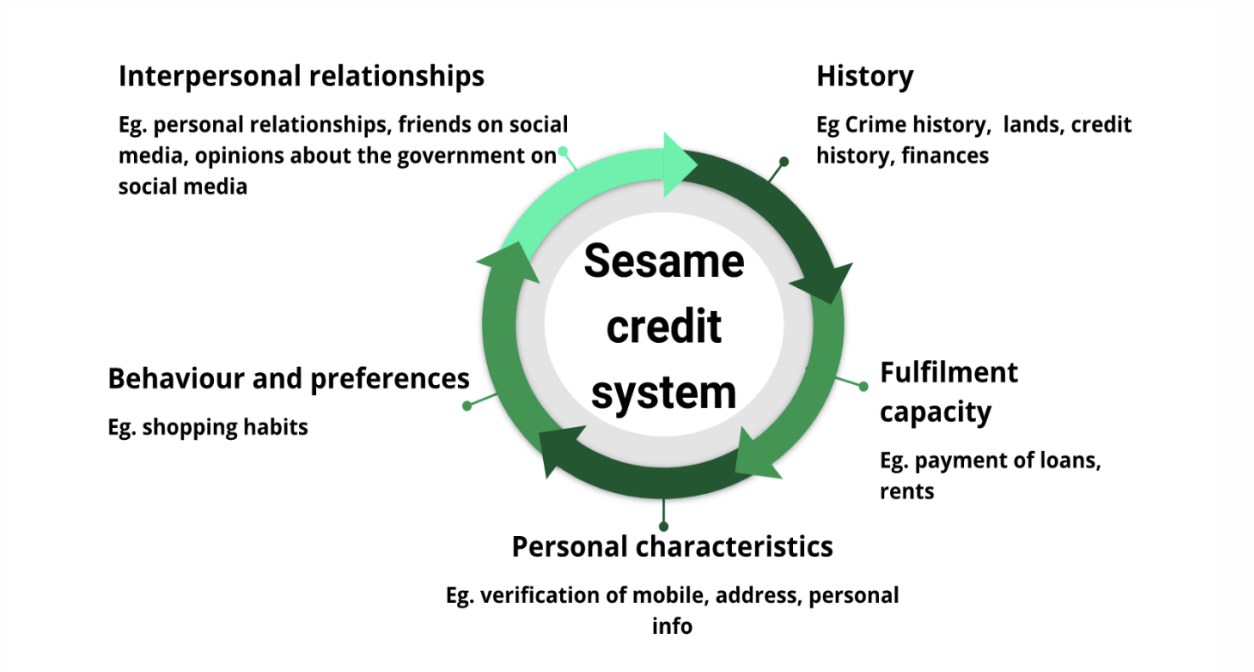


Figure 1. Sesame Credit System [5]

The diagram above reveals the five aspects of the Sesame credit system: history, fulfilment capacity, personal characteristics, behavior and preferences and interpersonal relationships. It also includes examples of what the algorithm takes into account when calculating the individual social score such as a citizen's credit history, financial purchases, their behavior towards friends and family and their opinions towards the government will be tracked and measured to create a score [5].

What would the outcome be if the U.S. were to adopt a system that had elements of the current FICO® system and China's social credit system? A possible implementation of this system might be launched as a pilot program at first, would be cyber centric and similar to a FICO® score. A FICO® score represents the probability a customer will default on a loan or other form of credit. The new scoring system might assign individuals a numeric value based on their susceptibility to a cyber-attack. This would essentially make cyber trust worthiness just as important as credit worthiness.

The cyber trust score for an individual in the U.S. could be associated with a unique ID like a social security number. When it comes to financial credit scores there is a benefit to the consumer because it can be used to grant access to financial instruments not otherwise available. Credit scores can make life easier with good scores and be a great tool as they reward past positive behavior with lower rates on future loans or greater access to credit. But if an individual's identity is stolen and abused or a creditor of records miss-reports a serious transaction, scores can be erroneous and misleading. For a credit score to not become a drag on access, individuals must keep track of all purchases, not spend outside their means, pay off balances in a timely fashion, and monitor their accounts for fraud.

It would be a similar scenario for the cyber trust score. Individual's scores might be based upon personal internet usage, an individual's propensity to interact with malicious sites or files, the security hygiene of their devices, and possibly even the integrity of their blogs, number of social media friends or posting "likes". All in all, the platform would be designed to create a measure of cyber worthiness; a measurement of one's potential for being a cyber risk.

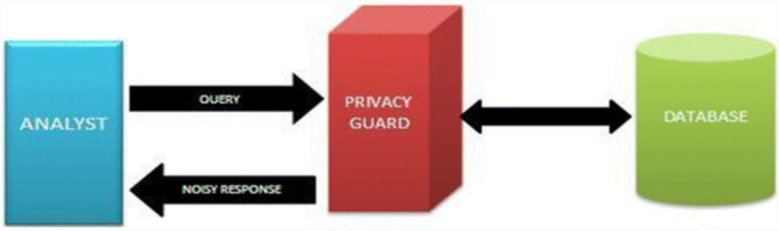
While such a scoring solution may be technologically viable, gathering the necessary data causes privacy concerns. Should a person's online habits be allowed to be monitored as a means of granting access to systems and data; information? Would access only be achievable by "opting-in" and keeping one's surfing nose and desktop clean. Would the internet no longer be a place for discovery and free speech? Could it actually become a place of censure? The answers to these questions will be driven by data collection solutions chosen in this emerging area of technology.

Privacy Technologies for Trust Scoring

User identity could also be protected by privacy-enhancing technologies (PETs). Systems could be developed to analyze data through AI via pattern analysis, which would work by using a pattern-based query that is focused on a specific, uniquely identifiable individual or individuals [13]. In 2017, Apple Inc. started a massive experiment with new privacy technology aimed at figuring out a way to build products that understand users without invasively monitoring their activities.

Differential privacy seeks to obscure data so that the true identity of a user associated with the data is unknowable. Data being analyzed can be obscured through an interface system that adds measurable amounts of statistical noise necessary to make it sufficiently difficult for someone without proper authorization to tie back certain data to a particular user. In this case, the issues of privacy may be avoidable [9]. To explain how differential privacy works and how it would solve the privacy issues that a cyber trust score for individuals would bring, the following excerpt is from The Journal of Big Data, Article #15:

Figure 2 shows the differential privacy mechanism. The analyst sends a query to an intermediate piece of software, the Privacy Guard. The guard assesses the privacy impact of the query by making use of a special algorithm. Then, the query is sent to the database by the guard getting back a clean answer based on data that has not been distorted in any way. The guard then adds the appropriate amount of "noise," scaled to the privacy impact, accordingly making the answer uncertain to ensure the confidentiality of the individuals whose information is in the database and sends the modified response back to the analyst [9].



Differential privacy mechanism [1]

Figure 2. Differential Privacy Mechanisms

Additionally, Immutable audits can be utilized to keep logs of when data is accessed, by whom they are accessed and when they are altered. The audit records themselves can be protected from alteration.

But differential privacy and AI-based PETs are not perfect solutions. They can suffer from entropy balance and bias. Furthermore, for such solutions to solve all privacy concerns associated with cyber worthiness scoring, privacy guards would have to be placed in front of every transaction database and log store imaginable. Agreements would have to be negotiated between system owners and scoring companies. Finally, all of this would have to be policed. Imagine the policy and process infrastructure necessary to authorize privacy guards and assure fair access.

3.0 Implications

Technology

According to research conducted by Tufts University alongside Mastercard done in 2017 on 60 countries, people across the globe are becoming increasingly dependent on, and distrustful of technology simultaneously. This paradox is a global phenomenon and accurately describes the current landscape for cloud adoption and migration. In many ways, industry is moving systems to the cloud with good intentions only to discover gaps in business processes and skills that create security vulnerabilities. As we devise cyber scoring approaches, great care should be taken to understand the potential shortcomings that adoption could bring.

An immediate area of concern surrounds the algorithms necessary to make cyber trust scoring work. Algorithms should not be made that artificially hinder access. AI algorithms may have bias do to the fact that the data used to train them has bias. Industry would need to come to consensus on what information the individuals monitoring and analyzing the data being gathered would be able to see. Industry would need to figure out who would be monitoring and aiding the machine learning algorithms to ensure objectivity, accuracy, and sensibility, if even possible. There has already been concern around personal digital assistants such as Amazon's Alexa or Google's Assistant, and those who analyze the commands given to help make *her* more intelligent and well cultured.

Social

The social credit systems in China encourage behavior that is deemed legal and acceptable by the Chinese government. The social credit systems gives points for acts of kindness such as making charitable donations or taking an elder to the doctor. Due to China's rapid shift from agrarian to postindustrial society they lack and require an established framework for unknown parties to determine each other's trustworthiness. China has a history of authoritarianism and is attempting to use this system to maintain control. Drawbacks of the social credit system are that Chinese citizens are punished harshly for bad behavior that the Chinese government wants to discourage. These punishments can range anywhere between travel bans, public shaming, slower internet connection, and rejection from high visibility jobs or higher quality education.

If people that are in your network are being punished and going against what the government considers proper and positive behavior, your score and lifestyle may be impacted negatively. The most daunting part is that the punishments are occurring outside of a legal system without a presumption of innocence, a jury, or a trial. Some people may believe that the Chinese are using this surveillance system to oppressively modify the behavior of their citizens which is uncomfortably reminiscent of 1984, by George Orwell and Nose Dive, by Netflix's Black Mirror Series.

Similar to the social credit score in China, the cyber trust score system would be able to create a blacklist before hiring people or giving them contracts related to national security or senior industry jobs so that there would be less risk of attack to vital entities of the economy and the government. The cyber trust score system could possibly impact society positively because individuals would be more cognizant of how they interact with other people through connected devices. People would take more precaution when posting content to the internet and be more concerned about what would be tracked and what would not be and as a result, cybercrime would have a less detrimental effect on the economy, society, and livelihoods of individuals because individuals that would have become cybercriminals would commit less crime because of the fear of putting their score and therefore, their livelihood at risk. By giving somebody a personal score and telling them if they are doing good or bad, they can begin to understand what it means to them and will start to view their cyber habits in a way where it reflects on them as a responsible contributing member of society.

One of the major hurdles a cyber trust scoring system faces would be that industry would need to figure out how to encourage individuals to achieve and maintain a high cyber trust score. While it would not be just for the U.S. to penalize individuals for not having a predefined baseline cyber score, the current financial credit score penalizes those who do not have above a certain score by making it increasingly difficult for the person to make large purchases and participate in society with such convenience. Industry would need to figure out if there would be an alternative, other than being completely off the grid by choice if the cyber trust score system was implemented.

Policy

Policy implications abound with the implementation of a cyber trust score in the United States. Currently, our credit scores are created by private companies not the government. With that said, government agencies are allowing corporation to consider additional factors in addition to credit scores. The New York State Department of Financial Services announced in 2019, that life insurance companies are now allowed to base premiums on what they find in your social media posts [7].

A company called Patron Scan sells a kiosk, desktop, and handheld system that is designed to help bar and restaurant owners manage customers by maintaining a list of objectionable customers designed to protect venues from people previously removed from other premises due to fighting, sexual assault, drugs, theft, and other negative behavior. Patron Scan uploads a public list that is shared among all Patron Scan customers which is similar to the black list that the Chinese use and is often used by Patron Scan customers for access control [7]. AirBnB, a Patron Scan customer and a major provider of travel accommodation has more 6 million listings in its system. It bragged that a ban from AirBnB can limit an individual's travel options. According to their policy, AirBnB can disable your account for life for any reason it chooses, and it reserves the right to not tell you the reason [7].

It would be a similar situation with the Cyber Trust Score system but perhaps, there could be an appeal process. It is the same situation with Uber, under a new policy announced in May of 2019: if your average rating is "significantly below average," Uber will ban you from the service, if given a low cyber trust score you could be banned from certain Internet privileges. WhatsApp may not have a high utilization rate in the United States but in other parts of the world, the platform have more power and influence as it serves as the primary vehicle for digital communication. WhatsApp also bans users if it distrusts them [7].

If the trends continue, it is possible that in the future a majority of misdemeanors and even some felonies will be punished by corporations instead of the government. Washington, D.C. would not be the powerhouse anymore, Silicon Valley would be. It is a slippery slope away from democracy and toward corporatocracy. This is exactly why we need a system of checks and balances, continuously validating and questioning our loyalties and dependencies on technology and the firms that create them.

Regulatory

Since the 1890's, the idea of a "Right to Privacy," has evolved as technology and society have evolved. Initially, the right to privacy was viewed as a "right to be left alone" and undisturbed [3]. Till today, on the individual level, the effect of a privacy violation is relatively the same in the sense that the individual would still feel a loss of pride and extemporaneity, as well as a threat to their freedom and their right to privacy.

Recently, there has been more pressure to tailor data protection laws to the innumerable circumstances in which they are applied. Over fifty organizations have joined forces to create the Principles of Fair and Accurate Security. The Principles of Fair and Accurate Security mentions transparency into the methodologies, appeal and dispute resolution processes, and that the ratings should be empirical, data-driven, or based off of an expert opinion [16]. It also covers the significant change process, the nuances of commercial agreements, how ratings will be appropriately protected and that rating companies should not publicize an individual

organization's rating or provide third parties with sensitive or confidential information on rated organizations that could lead directly to system compromise [16].

The EU General Data Protection Regulation (GDPR) can be used as an example of data protection regulation adapting to the challenges of technology, giving the data subject increased control over their personal data whilst providing necessary flexibility in its implementation.

The biggest caveat to individual cyber trust scores is that no matter what, there will be privacy concerns and violations. When it comes to developing cyber trust ratings for individuals it gets very complicated and uncomfortable because technology rating systems are typically invasive. There is always the risk that citizens will feel distrusted and uncomfortable under surveillance, thus diminishing their trust in government or industry.

4.0 Recommendation

Today we are at the crossroads of trust as traditional domain-based approaches are obviated by cloud adoption and zero trust architectures. For it all to work, cyber trust scores for individuals and entities may become the next measure for granting access to system and data. Is it possible a whole new industry for measuring cyber trust could evolve? Would it be modeled after the credit scoring industry created by Equifax, Experian, and TransUnion?

Technologists are responsible for solving difficult problems. Cyber trust scoring can have significant social, policy, and regulatory implications and today's technology solutions may not cooperate. Monitoring user behavior raises many privacy concerns. Automation can cause bias and differential privacy techniques require extensive inter-connectivity and complicated obfuscation algorithms.

Accordingly, it is recommended that Industry and government work diligently together to address the gaps that need to be addressed before cyber trust scoring in America become a reality.

5.0 Bibliography

[1]. Agre, Philip E., Rotenberg, Marc "The New Landscape." *Technology and Privacy: The New Landscape*, MIT Press, https://pages.gseis.ucla.edu/faculty/agre/landscape.html.

[2]. Brieger, Kelly, Sift Science Launches Digital Trust Platform™ – Holistic Approach Boosts Customer Loyalty and Retention, EconoTimes 1 Nov. 2017 https://www.econotimes.com/Sift-Science-Launches-Digital-Trust-Platform--Holistic-Approach-Boosts-Customer-Loyalty-and-Retention-982321

[3]. Britz, J. J. "TECHNOLOGY AS A THREAT TO PRIVACY: Ethical Challenges to the Information Profession." *TECHNOLOGY AS A THREAT TO PRIVACY: Ethical Challenges*, Department of Information Science University of Pretoria, http://web.simmons.edu/~chen/nit/NIT'96/96-025-Britz.html.

[4]. Broeckelmann, Robert. "Authentication vs. Federation vs. SSO." *Authentication vs. Federation vs. SSO*, Medium, 24 Sept. 2017, https://medium.com/@robert.broeckelmann/authentication-vs-federation-vs-sso-9586b06b1380.

[5]. Botsman, Rachel. "Who Can You Trust?: How Technology Brought Us Together – and Why It Could Drive Us Apart" Penguin Books Limited, 2017, 5 October 2017 https://books.google.com/books/about/Who_Can_You_Trust.html?id=7cGWDgAAQBAJ

[6]. Day, Jamison. "Cyber Threat Scoring Is Not Risk Assessment: LGC." *Cyber Threat Scoring Is Not Risk Assessment*, Looking Glass Cyber Solutions Inc., 10 Oct. 2018, https://www.lookingglasscyber.com/blog/tech-corner/cyber-threat-scoring-not-risk-assessment/.

[7]. Elgan, Mike Uh-oh: Silicon Valley is building a Chinese-style social credit system, Fast Company, 26 Aug. 2019 https://www.fastcompany.com/90394048/uh-oh-silicon-valley-is-building-a-chinese-style-social-credit-system

[8]. Huang, Geoff. "Sift Scores: Growing and Protecting Businesses." *Sift Scores: Growing and Protecting Businesses*, Sift Blog, 1 Aug. 2019, https://blog.sift.com/2019/sift-score.

[9]. Jain, Priyank, and Nilay Khare1. "Differential Privacy: Its Technological Prescriptive Using Big Data." *Journal of Big Data*, SpringerOpen, 13 Apr. 2018, https://journalofbigdata.springeropen.com/articles/10.1186/s40537-018-0124-9.

[10]. Ma, Alexandra. "China Has Started Ranking Citizens with a Creepy 'Social Credit' System - Here's What You Can Do Wrong, and the Embarrassing, Demeaning Ways They Can Punish You." *Business Insider*, Business Insider, 29 Oct. 2018, https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4.

[11]. Mims, Christopher. *The Secret Trust Scores Companies Use to Judge Us All: BAK Message Board Posts*. The Wall Street Journal, 6 Apr. 2019, https://www.wsj.com/articles/the-secret-trust-scores-companies-use-to-judge-us-all-11554523206?mod=hp_listb_pos1.

[12]. Reiter, Andrew. "The Role of Trust in Technology." *THE ROLE OF TRUST IN TECHNOLOGY*, Shield AI, 19 Dec. 2018, https://www.shield.ai/content/2018/12/19/the-role-of-trust-in-technology.

[13]. Rosenzweig, Paul, and James Dempsey. "Technologies That Can Protect Privacy as Information Is Shared to Combat Terrorism." *The Heritage Foundation*,

https://www.heritage.org/homeland-security/report/technologies-can-protect-privacy-information-shared-combat-terrorism.

[14]. Saltonstall, Max, Google Beyond Corp with Max Saltonstall, Software Engineering Daily, Apple Podcasts, 25 Sept. 2019, https://softwareengineeringdaily.com/2018/02/09/google-beyondcorp-with-max-saltonstall/

[15]. Tech Target Network, Search Security definitions https://searchsecurity.techtarget.com/definition/federated-identity-management

[16]. "Transitive Trust." *IBM Knowledge Center*, https://www.ibm.com/support/knowledgecenter/SSLTBW_2.4.0/com.ibm.zos.v2r4.euvfa00/euv2b3_Transitive_trust.htm.

[17]. U.S. Chamber of Commerce, Principles of Fair and Accurate Security Ratings https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings

[18]. Waterman, Shaun. "A FICO-Style Score for Companies' Cybersecurity? Some Say It's an Idea Whose Time Has Come." *CyberScoop*, CyberScoop, 8 Aug. 2017, https://www.cyberscoop.com/insurance-regulators-pitched-fico-style-score-cybersecurity/.

[19]. Weber, Steven. "FICO Offers Free Cybersecurity Ratings to Companies Worldwide." *FICO*, FICO FRAUD & SECURITY, 27 June 2018, https://www.fico.com/en/newsroom/fico-offers-free-cybersecurity-ratings-to-companies-worldwide.

[20]. Webster, Teri. "Apple Quietly Implements 'Trust Scores' Based on Users' Phone Data." *TheBlaze*, TheBlaze, 13 Dec. 2018, https://www.theblaze.com/news/2018/09/21/apple-quietly-implements-trust-scores-based-on-users-phone-data.

[21]. Zaidiaiman. "China's Social Credit System – Analysis of a Socio-Technical Controversy." *Master Tsinghua Data Science and Expertise*, 30 Apr. 2018, https://mastertsinghua.wordpress.com/2018/04/30/chinas-social-credit-system-analysis-of-a-socio-technical-controversy-by-cassandre-de-froidmont-ludovica-donati-miriam-steffen-and-aiman-zaidi/.

[22]. Rose, Scott, Borchert, Oliver, Mitchell, Stu, and Connelly, Sean. "Zero Trust Architecture" *Draft NIST Special Publication 800-207,* National Institute of Standards and Technology, September 2019, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft.pdf