September 2016

National Institute of Standards and Technology (NIST) Request for Information:
Information on Current and Future States of Cybersecurity in the Digital Economy

Prepared by:

Trusona, Inc.
Scottsdale, AZ
https://www.trusona.com

Trusona Introduction

Trusona is the world's first and only insured cloud identity suite designed to guarantee the true persona behind the most sensitive online transactions across the enterprise. Trusona's cloud identity suite offers a multi-factor authentication infused by identity-proofing and includes three levels of service:

- **Essential** – designed for consumers and is FREE as our gift to the world
- **Executive** – designed for enterprise use
- **Elite** – designed for VIPs and Critical Assets – the only solution backed by an A+ rated insurance carrier

Trusona protects the world's most sensitive assets including; SWIFT wires, DTC stock transfers, critical infrastructure logins, government systems, high net-worth individual accounts, VIPs and major news social media, Business Email Compromise (BEC) wire fraud, healthcare records, and much more.

Executive Summary

Trusona is providing commentary on the four following RFI topics:

1. ! Critical Infrastructure Cybersecurity
2. ! Cybersecurity Insurance
3. ! Cybersecurity Research & Development
4. ! Public Awareness & Education

Critical Infrastructure Cybersecurity

Current and Future Trends

We see news on an alarmingly regular basis of power plants, water systems etc. being breached. If existing vulnerabilities in the institutions we rely on for the most basic elements of our lives aren't addressed, we may be headed for an e-9/11.

The stakes for obtaining 100% certainty of who is on the other end are considerably higher in any interaction that involves critical infrastructure operators. However, there is very little hard data and limited understanding and identity controls within critical infrastructure today.

Immediate Action Needed

Trusona is the category-defining identity and authentication platform for the world's most critical use cases, i.e. Critical Infrastructure. Trusona Elite is the only insured identity authentication solution to offer in-person identity-proofing, secure distribution of a TruToken that exceeds the current, published National Institute of Standards and Technology (NIST) level 4 standards. Additionally, each Trusona solution includes patented anti-replay technology so it is immune to highly sophisticated session replay attacks.

Protecting Critical Infrastructure is a matter of life and death and requires 100% certainty and insurance – something that to-date has been impossible online. Critical infrastructure must utilize an insured solution that is based on actuarial data and includes in-person identity proofing.

Trusona’s core technology has experienced zero fraud in over 119 million transactions to date, allowing Trusona to provide 100 percent security assurance backed by actuarial data.

Trusona has designed a formula to showcase what is needed for cybersecurity solutions to insure their results. You can read the published, technology agnostic whitepaper here:
https://trusona.com/wp-content/uploads/Trusona_Insurance_Formula_v4.pdf

Cybersecurity Insurance

Current and Future Trends

Cyber-attacks are now so frequent that they border on uninteresting. And as attacks have increased in the past few years, so has the number of security startups claiming to tackle the problem.

Security, like most other traditional infrastructure systems, is fast becoming outdated as computing becomes decentralized, even extending to remote and mobile users across the globe. Traditional defenses no longer work as hackers long ago outsmarted them, creating a constant cat and mouse chase for the industry to catch up with the criminals. Further, this lag in security is exacerbated by a convergence of new forces like the Internet of Things and the big data explosion. Now, human behavior, especially in the workplace, is immersed in technology, leaving CISOs to scramble to address existent problems as well as newly introduced risks.

It is not enough for a vendor to tell consumers they are the best; third party validation is required to cut through the noise and prove what solutions can actually hold water. Security companies need to prove their efficacy and have some skin in the game themselves. Most large organizations have some form of cyber insurance from third party insurers, but this insurance only has value *after a breach*. Companies need a solution strong enough to *prevent losses in the first place*. We need to turn the tables; take control away from the cyber criminals and bring a game-changing advantage to the businesses We need security solutions so powerful that a third-party insurer is confident enough to back the companies assertions of unmatched protection.

Immediate Action Needed

Trusona is the first and only identity platform and authentication solution powerful enough to be insured by an A+ Rated Insurance Carrier. Trusona offers up to $1MN insurance per financial transaction. Trusona’s identity suite is designed to guarantee the true persona behind the most sensitive online transactions across the enterprise.

Trusona has designed a formula to showcase what is needed for cybersecurity solutions to insure their results. You can read the published, technology agnostic whitepaper here:
https://trusona.com/wp-content/uploads/Trusona_Insurance_Formula_v4.pdf

Cybersecurity Research and Development

Current and Future Trends

Businesses are up against very motivated cyber criminals. These criminals are constantly finding new and inventive ways to conduct fraud and they are stealing billions a year from American businesses. Anyone who reads the news is aware of a new data breach on a daily basis. In order to combat these ever-changing attacks, cybersecurity solutions need to be as innovative as the criminals. There is no room for complacency. There is no room for status quo.

Immediate Action Needed

The Trusona team is dedicated to shedding light on the darkest corners of the Internet. We are committed to making the Internet a safer place. This means we are constantly innovating new ways to combat the fraudsters. Every cybersecurity company must have a lab with employees dedicated to researching the latest fraud techniques and rapidly finding ways to ensure their customers remain protected. We must not be afraid to constantly change the way we think about security. We must not be afraid to make radical changes. Fighting today's cybercriminals requires constant research, development and motivation.

Public Awareness

Current and Future Trends

It is imperative that consumers understand the risks of conducting business online. Companies can deploy a myriad of cybersecurity solutions but if consumers keep opening themselves us for attack it will be a losing battle.

We know that consumers want to be secure but they also want their online experience to be easy and convenient. Security and convenience are often at odds. We need solutions that can blend convenience and security to increase public adoption.

Yes, we must continually strive to educate consumers on the best practices for safely conducting business online. But the onus must also be on solutions to ensure we utilize effective security solutions that fight the real problem vs simply putting on a band-aid.

Immediate Action Needed

First, we need to move away from static technologies that only provide an appearance of security – such as passwords, SMS and Biometrics.

NIST's recent call to eliminate the use of SMS is a great step in the right direction. Fraudsters can reroute SMS in less than 60-seconds.

Likewise, biometrics are futile. While they give the appearance of security, a fingerprint scan, for example, is really just converted to a static credential. Fraudsters steal any static credential and simply replay the session data and businesses have zero way to know the difference between the criminal and their legitimate customer.

Trusona has launched the **#NoPasswords Revolution** to educate both businesses and consumers on the insecurity of passwords (and any static credential for that matter). Passwords were invented in the early 1960's and have not had one single innovation since. They were created for access management and were not intended to be the main line of security and authentication when wiring millions of dollars. We must move on and use real technology to combat the problem.

We have published our #NoPasswords Manifesto to help educate businesses and consumers on the danger of passwords and encourage the dawn of a new day – a day without the use of the antiquated technology. You can read the manifesto here: https://www.trusona.com/manifesto/

Additionally, Trusona conducted a survey of 250 consumers' password habits. The results show a disturbing trend between consumer trust and ignorance: nearly all of survey respondents said they trust passwords as an effective security measure, and that group of consumers was shown to have the worst habits in password use. When all hackers need to access an entire corporate network is a single password, everyone is responsible for making sure consumers are educated on the risks they're taking every day—not just for themselves, but for the entire internet. A brief overview of the survey results are below:

Blind Trust: Customers Aren't Always Right

"If I had asked people what they wanted, they would have said faster horses." — Henry Ford

- Per a recent report, 63% of data breaches in 2015 were the result of weak, stolen or default passwords.
- 83% of consumers surveyed said they have at least a high level of trust in passwords as an effective security measure
- On average consumers have more than 10 services with logins, but only use between 1-5 passwords across all of them
- One in three consumers doesn't change their passwords are being notified of a data breach

Convenience Trumps Security

- 60 percent of consumers take no action to keep their data safe, while 50 percent actively disable two-factor authentication that business put in place
- Only 11 percent of people use a dedicated password manager, while almost one-third write their passwords down on a piece of paper and half of consumers rely on their memory to keep track of passwords
- One in six consumers shares their passwords on a regular basis

Passwords Cost Businesses In More Ways Than One (customer attrition)

- Having an inconvenient login process equals lost business. While consumers think passwords are fine they also have little tolerance for the issue.
    - 30 percent will stop doing business if they have trouble accessing their account
    - 40 percent have already discontinued use of a service simply because they forgot their password
- According to Gartner, 30 percent of call center volume is about password reset, while Forrester states that the average cost of a call center all is $25

Passwords Are Super Annoying

In the past 30-days alone:

- Two-thirds of consumers have forgotten one or more passwords, while 60 percent have had to reset at least one password and 40 percent have been locked out of an account

Join The #NoPasswords Revolution

"I am not saying it's going to be easy, but I am saying it's going to be worth it" —Moffat Machingura

- 67 percent of consumers had a positive reaction toward the idea of a password-less login that also increased security
- Over half the respondents would jump for joy if they were given the option to login without passwords

**The survey was conducted and analyzed by SSI in August 2016*