# Request for Information

## Submitted to the Commission on Enhancing National Cybersecurity


| | |
|---|---|
| Respondent Organization: | CynjaTech<br>P.O. Box 65916<br>Washington, DC 20035<br>info@cynja.com |
| Information Prepared By: | Heather Dahl<br>Chase Cunningham |
| Date Submitted: | September 9, 2016 |

# Information on Current and Future States of Cybersecurity in the Digital Economy

## Executive Summary

### The Internet & its Promise

The Internet has revolutionized the way we live our lives, it seems to touch us in every aspect from our personal relationships to business and even our health. Many consider the Internet to be one of the most important innovations. It has brought society advancement, growth and connected us on a global scale.

It's because of the Internet that we have become a digital society. A digital society that is now inseparable from our physical world. This digital society is only in the early stages of maturing.

### It's Fraying

Today's Internet is demonstrating signs of straining, potentially to a breaking point. We don't have to look far for evidence of this. News headlines of another data breach are a regular occurrence; from the Democratic National Committee to the Office of Personnel Management or Sony are evidence of this trend. These continual breaches have created an expansive and growing cybersecurity industry. The U.S. Federal cybersecurity market alone is $18 Billion is expected to grow at a steady Compound Annual Growth rate of 4.4 percent.[1]

Today there are armies of IT professionals working on cybersecurity related solutions. The vast majority of them are either focused on tools to try to keep malicious invaders out of networks or performing forensic analysis after they failed. These are critical functions but they do need improvement. However, much of our focus as an industry is dedicated only to developing reactive and defensive solutions. As a result, we are not fixing the problem of insecurity, we are creating more bandages to cover weaknesses and this has lead into what is best described as an arms race against the malicious players.

### Think Differently

CynjaTech is thinking about the problem differently. As a society, we need to acknowledge that our life is now a digital one. We can no longer think of cyberspace as an alternate reality or an existence separate from each one of us.

---

[1] Market Research Media, U.S. Federal Cybersecurity Market Forecast 2017-2022, September 5, 2016

Our digital society is inextricably intertwined with our physical lives. When we are harmed in either the digital or physical world we are hurt for real. We can see this when teens commit suicide from being bullied online or kids are abducted as the result of a chat app or even when medical devices that provide life support are hacked in health facilities. The examples of how lives are harmed by digital attacks grows by the day.

## Key Problem Areas

- Data Ownership & Management
- Rules & Regulations
- Technical Education
- Cyber Education.

## Forging a New Frontier

Today our digital world is metaphorically the Wild Wild West. Our challenge now is to set up a society where we can live with safety and full protection of our individual rights. That's why we need to approach the notion of cybersecurity from a new understanding, one that will actually benefit society rather than temporarily patch security flaws. We must look towards a new cybersecurity that will support how we actually live and engage with our digital neighbors.

*Best practices need to change:* Organizations, including business, government, and technology firms, need to stop physically holding data of their customers, clients, or individuals who need to access their services. They should stop sucking up and hoarding every piece of data they can get their hands on. The risks to our security and ultimately rights as a society far outweigh the benefits.

*Digital rights must be carefully considered:* As a democracy we need to look at what data ownership, data control and privacy means in a digital society. Our federal, state and local policies in this area are lagging. Businesses who profit from our digital lives are the ones leading the way in defining our individual rights in a digital democracy. As a result, our rights as an individual are being left behind. More entities need to be involved in defining the boundaries around our digital artifacts and property. And technology must be created to support those rights and policies protecting us.

*Personal responsibility in our digital lives:* The fact is, we are all connected. While the benefits of this connectivity means it's easy to conduct business on a global scale or share details of our lives with friends across the country, it also means that when we fail to take security precautions we expose our networks to the same risk. Critical thinking about our personal responsibilities online is a major deficiency. Approachable conversation, education and resources about our personal responsibilities in cyberspace must be a part of every aspect of our lives from home, to work and school. Just like in public health, we've educated the general population on the importance of washing their hands, we need to approach digital responsibility the same way. Given that our lives are now digital, we all need to understand how to live safely in this world.

*Educating for success in this digital world:* Technology is core to our society but we face a shortage of skilled workers, especially in cybersecurity. Much focus has been placed on coding camps for schools and kids. Those are important and valuable programs. But the fact remains, not all kids will grow up wanting to work in technology, yet they will use technology. We must rethink our approach to cyber education. It needs to expand beyond this current focus on programming skills or cyberbullying because the fact is not every adult will need or want to program, nor is cyberbullying the only digital threat they will face. Now is the time to teach digital life skills that spans technology, critical thinking and even our civic responsibility in cyberspace.

### New Thinking

The exponential growth of cyber crimes, data theft and database breaches, show that the Internet which powered so much benefit has also placed many of us at an increased risk that didn't exist 20 years ago. The traditional cybersecurity of today is providing some protections but obviously not solving the underlying problem. The time has come for government to support and encourage those technologies which approach solving today's problems in a different way—that of prevention and education.

CynjaTech is taking a new approach to cybersecurity. We are a technology firm focused on securing families, children and senior citizens online. Rather than building the next in a long line of *better* defensive solutions, we look at how to improve lives in a digital society. Our security technology looks at technology being a part of our daily life, not a separate virtual reality or another cool app, but rather something that touches us at every moment of the day.

Our firm solves data management *and* cyber education together in our platforms. We are leading the way in a new generation of technology firms that will prevent exposure to cyber crimes and empower individuals to protect their digital lives and communities. We are dedicated to developing technologies that will protect our most exploited populations online because they have not been provided with the help they need online.

We focus our comments on these key problem areas; Data Ownership & Management, Rules & Regulations, Technical Education and Cyber Education. These fall into the Enhancing National Cybersecurity Commission's core topic areas of Cybersecurity Research & Development and Public Awareness & Education.

## Current and future trends and challenges in the selected topic area;

Today's Internet was born out of early innovations that established the most resilient network on the planet. This resilience comes from the protocols invented during the late 20th century. These protocols established mechanisms that enable

decentralized and distributed communication. Since these core protocols do not depend on centralized services they have no single points of failure.

While this was a great innovation that has led to not only the Internet being an immense driver of economic activity, it has ushered in the beginnings of a digital society. However, the Internet is facing problems. Those protocols focused on resiliency they did not focus on security and they did not focus on identity. We didn't plan for our lives to become digital as they have become.

The problems are well known. We hear about data breaches constantly. The news headlines we all hear–the Sony compromise, the Office of Personnel Management breach, the Democratic National Committee hack—are, sadly, all too real and devastating. However, the headlines obfuscate the sheer amount of data being stolen in what amounts to be millions of data records. Eight months into 2016 and we have seen 638 breaches[2] so far and there is no end in sight because cyber crime around the world continues to grow exponentially.

The fact is, it is our data being stolen. The data of citizens, kids, senior citizens, families, it is the data of humans with real lives who have little control over how their data is protected in the first place. Technology has reversed the course of personal ownership and now a system has been created that means our data is no longer ours and the security of our data is someone else's responsibility.

> Moreover, Americans have low levels of trust in the government and business sectors that they associate with data collection and monitoring. They are not sure their core communications channels are secure, and they have exceedingly low levels of confidence in the privacy and security of the records that are maintained by a variety of institutions in the digital age. Indeed, noteworthy numbers of them have suffered privacy breaches, especially younger adults.
>
> *Privacy and Information Sharing, Pew Research Center, January 14, 2016*

The trend until now has been to take away an individual's digital rights and then leave the individual to clean up the aftermath in their own lives as a result of a cyber crime. There remains futile accountability for how organizations, businesses or agencies share, treat or protect our data.

With the hype around data mining, analytics and monetizing our data, there is also little incentive at the moment to provide individuals with the ability to control their data. This means data is stored and copied in centralized silos and is at constant risk of compromises, leaks, attacks, and behavioral tracking because hacking the single key used in this architecture unlocks everything. With this model, an individual's data is then replicated with each app, piece of software or website that they use making it virtually impossible to control it, let alone provide the individual an efficient way of consenting on how, or if, they want to share their data. In today's technology, and much of the future technology that large vendors

[2] http://www.idtheftcenter.org/images/breach/DataBreachReport_2016.pdf

propose, data is owned by everyone but the individual or organization who truly has the inherent right to own it. The advancement of technology has left individual rights behind and as a result it has created a costly cybersecurity quagmire.

The many data breaches and hacks which leads to millions of pieces of data, data representing citizens, not only provides the necessary fuel for malicious actors to commit crimes hacking, espionage, or surveillance, it also enables identity theft, harassment, stalking, and unwanted sexual solicitations enabling bad actors to pretend to be trusted members of our lives. This is especially dangerous to our young and old.

These problems have also sparked an arms race of sorts. The cybersecurity industry has been growing at a high rate. Gartner Research reported the global cybersecurity market will be worth $170 Billion in the next four years.[3] We have seen much advancement in the areas of security. Private industry is producing more and more tools that improve on the security of devices and systems. This is progress but it is largely defensive solutions to keep people out and to better identify when people break in.

Where there has been less investment and focus is on addressing the broader issues related to what it means to be a digital society. It is evident that we no longer can treat the Internet as an alternate reality. We have one life and that life exists both physically and digitally at the same time. Whether we are harmed digitally or physically it directly impacts our life. As such we need to start thinking differently about the problems we face today.

We need to address issues such as:

**Data Ownership & Management:** Technology firms and businesses have been defining data ownership to meet their interests. It is time for legislative and policy-making bodies to begin looking at data from the rights of an individual and populations, like children and senior citizens, whose voice is often overlooked. Should digital data be treated as property? Should individuals be able to retain rights over their data? Should individuals and organizations be able to share their data but still retain rights and ownership of the data being shared? If so, should we reduce or control the amount of data that is copied and replicated into the databases of others? Should others that need access to our data request it rather than horde copies of it? Limiting data duplication ought to improve security as it reduces the number of opportunities from which it can be stolen. This is a dialogue that must begin in now.

**Rules & Regulations:** Now that we have become a digital society we need to start considering new social norms – norms embodied in our rules, regulations, laws as well as social etiquette. Interacting with others whether socially or

[3] http://www.gartner.com/newsroom/id/3135617

transacting business ought not be very different from a policy standpoint than it is in the physical world. We need to look at establishing boundaries for how we should interact together; boundaries that are embodied within new and updated policies. How should those boundaries be established? Are these boundaries similar to the rules, regulations and laws that have been established in the physical world? We need to start these conversations.

**Technical Education** – Throughout history, when society went through great innovation transitions it became critical to ensure that there were enough skilled workers to support the new technologies. Cyberspace is no different. Given that we are in fact a digital society now; these skills are becoming mandatory. What can we do to ensure that more students are trained with the basic skills for this new world? How can we start training and exposing students at a younger age? How can we ensure that more people have the skills to support this new infrastructure that is cyberspace?

**Cyber Education** – While not everyone will be interested in or well suited for technical jobs within cyberspace, whether our children become doctors, small business owners, teachers or regardless of their profession—technology will be a part of their jobs and lives. We all need to understand how to live safely in this new world. In the past, much effort has gone into teaching people, young and old, how to interact in the world. We teach children how to behave in public. We teach people how to drive. We educate people on health issues such as preventing mosquito borne illnesses or sexually transmitted diseases. It is just as important that everyone learn basic skills to interact safely within the digital world. Each of us must take personal responsibility for our actions in both the digital and physical world. What does it mean to take personal responsibility in the digital world? How is this taught? When is it taught?

## Progress being made to address the challenges;

Progress is being made. We are seeing new and improved technologies in the defensive and investigative tools for cybersecurity. New armies of security specialists are building better intrusion detection devices, better forensic capabilities and collaborating more and more. This is great progress. Progress is also being made, albeit slowly, in the areas of digital identity and education.

We are witnessing:

**Data Ownership & Management:**

New technology that gives individuals, organizations and companies control over their data and the ability to secure it is beginning to come to market. It's being developed based upon a vision for the Internet which takes it back to its decentralized and distributed roots with no central servers and server farms. They are also introducing the capabilities where individuals, organizations and

companies can exert control and ownership over their data. They are launching peer-to-peer networks that rely on linked connections, encryption and identity to provide individuals the ability to explicitly and selectively share while retaining rights over their data. There are no central administrators with the single magic key, rather individuals maintain their own secure keys stored across networks. This same technology also limits the amount of data that needs to be copied into databases of third parties. Third parties will no longer need to retain copies of their customer's personal data. They will, instead, be able to ask the customer for it, when needed, by making a query to the customer's instance of their personal data.

Customer's always retain ownership and control over whether to share it in real-time. This same technology also limits the amount of data that needs to be copied into databases of third parties. Third parties will no longer need to retain copies of their customer's personal data. They will, instead, be able to ask the customer for it, when needed, by making a query to the customer's instance of their personal data. Customer's always retain ownership and control over whether to share it in real-time. This same technology also limits the amount of data that needs to be copied into databases of third parties. Third parties will no longer need to retain copies of their customer's personal data. They will, instead, be able to ask the customer for it, when needed, by making a query to the customer's instance of their personal data. Customer's always retain ownership and control over whether to share it in real-time.

Companies like Heuro Labs, Solid, MaidSafe, and CynjaTech treat customers like individuals who retain control of their personal data. It's an entirely new method for security and data management.

**Rules & Regulations:**

The ability for everyone – people, organizations, business – to exert control over their data is not only important in finding ways to limit the opportunities for hackers to steal it. It is also important in enabling a digital citizen's reasonable expectations of privacy.

The conversation over digital rights has been increasingly occurring at both public policy levels and within organizations and groups. Governments around the world are beginning to enact guidelines and regulations that is the start of establishing digital rights for citizens. The epicenter of these conversations began in Europe but it has also lately been occurring here like the debate surrounding the EU-US Privacy Shield.

One example of this in the United States is when Justice Sotomayor indicated that we may need to re-examine past doctrine regarding what makes up property. She wrote in the 'United States v. Jones,

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.
> …
> But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.
>
> *United States v. Jones, 565 U.S.___, Docket no. 10-1259 (2012)*

## Technical Education

Cybersecurity is a field that demands skilled professionals who possess the foundational knowledge, education and thought leadership necessary to confront the difficulties that accompany constant technological change. Advanced threat vectors, emerging technologies and a myriad of regulations require cybersecurity professionals to be skilled in technology as well as business and communications.

The numbers clearly show it's important we talk with boys *and* girls about cybersecurity as a career option. Sadly, according to the ISACA *2015 Global Cybersecurity Status Report*[4], 77 percent of women say that no high school teacher or guidance counselor mentioned cybersecurity as a career. For men it's 67 percent. That's why we, as a cybersecurity industry, need to expand our outreach because our efforts might be introducing a career path that no one else has mentioned as a possibility.

There are an estimated 410,000 to 510,000 information security professionals worldwide, and jobs are expected to increase 53 percent by 2018 with over 4.2 million jobs available. However, recent studies and reports suggest that there are simply not enough skilled professionals to fill them. With this disparity, it's clear there is a gap between STEM education offered in K-12 schools and the actual demand upon graduation.

Technical education is more than offering coding camp, designing a website or hosting a STEM weekend event. It's teaching teachers how to understand technology. It's giving our schools the digital tools needed to educate about technology, rather than another learning management system to track grades. It's helping kids learn about how the Internet works from the moment they enter

[4] http://www.isaca.org/Pages/Cybersecurity-Global-Status-Report.aspx

school, because the technical skills needed are more than what can be learned in an after school program.

**Cyber Education:**

Up until to now, general cyber education has been relegated to public service announcements with catchy taglines or a few basic lessons in our children's classrooms. That is not enough for all of us to navigate our new digital worlds successfully.

Cyber education must not only be a curriculum, it must become a part of the technology that we use. As we browse websites, download apps and use new software, technology firms can implement cyber education into the user experience. Sometimes, it's as simple as letting a person know the potential consequences of their actions and other times it is being transparent about their privacy practices and how that person's data will be shared or sold.

While cyber education campaigns focus on think before you click, many technologies are designed to get users to click before they think. It's a gap the tech industry must consider and they innovate the future of software and devices.

## The most promising approaches to addressing the challenges;

### Engineering Challenge

From an engineering perspective there is much work happening now to provide infrastructure for enabling Self-Sovereign identity. This term "Self-Sovereign" describes the concept of individuals, and businesses/organizations, being able to own their digital-selves – being able to own and control their data, being able to share it under revocable terms while still claiming ownership and control, being able to interact and collaborate with others while still retaining control over the digital assets that they have the rights to.

CynjaTech is one of the first developers to bring platforms, applications and services to market that treat customers as Self-Sovereign individuals rather than users. We're among the first in the world to develop technology that moves the Internet and its users into a decentralized network. The individuals and companies that participate in this decentralized network each own and control their own data. They are able to store their data wherever they choose and provide revocable permission to CynjaTech applications, such as CynjaSpace, access to the data to use our services. We never make copies of it – we are prohibited from doing so unless provided specific permission. We are eliminating today's security and privacy problems that resulted from today's centralized model.

CynjaTech is part of a growing list of developers who are committed to the concepts of Self-Sovereign Identity and the belief that people need to be able to control and take personal responsibility for their digital-selves. This development though is in very early stages of coming to market. The ecosystem still needs nurturing and support at many levels.

### Education Challenge

How can we create a cyberspace with training wheels for children that educates about making smart choices during every step of their early digital lives? Children learn how to ride a bike with their parents support and safety equipment so they survive any falls with minimal bruising. However in cyberspace, it's like we throw our children on motorcycles without helmets and hope for the best. Or we rely on technologies that are designed to fence in or spy on children without teaching them at the moment they make a poor choice.

At CynjaTech we believe cyber education must start at the moment a child taps a device. Given that toddlers are now online, it means we must not only offer education to kids but also their parents. These are conversations that today's parent never experienced growing up so we believe educational efforts to help parents navigate this world are just as important as educating kids in a classroom. Our technology brings the conversation directly to children, parents and educators through interactive tools, games and educational resources.

### Public Policy Challenge

In our nation's capital, more queries and clarifications are being issued asking technology companies practices surrounding collection, use and security of individual data. We can see a growing concern among legislators about how user data such as location, communications, and physical movement are being used, what precautions are being taken to protect this data and whether it’s being sold to third parties. As more is learned, the policy community will begin understanding the full extent how individual rights in our digital world has suffered and, hopefully, support technology that fixes the problem rather than those technologies designed to mask an exacerbating problem of data mining.

## What can or should be done now or within the next 1-2 years to better address the challenges;

### New Technology Innovations

Companies that are developing the next generation of security and data management platforms need financial support for research & development along with operating capital. Because the technology companies that dominate today

are built upon systems and business models that need a centralized database; this makes acquiring operating capital a challenge for those early stage companies trying to build a decentralized secure network infrastructure. Conventional wisdom means investors look for companies who are replicating the large companies models that exist today. Early stage companies that are trying to give people the ability to protect and control data are at a disadvantage when it comes to raising necessary capital.

## Supporting Education

Each day, the cybersecurity industry dedicates itself to protecting their client's most valuable assets. They spend countless hours focused on keeping data, intellectual property, systems and files out of the hands of cyber criminals. Their clients win and they win. But what are we doing about educating people—the individuals, each of us who use devices every day—about security? Not enough. You'll find corporate social responsibility programs that address the issue but education is usually relegated as a low tier activity with little financial investment.

Why is this important? All of us are experiencing the negative consequences of the Internet today. Maybe it's identity theft or our children downloading spyware into our family's devices. But unlike the industry's clients—who have budgets, IT managers, lawyers and executives demanding attention—individuals, families and children have no one at the corporate boardroom table demanding their security. Perhaps in the whirlwind of dollars and income statements, businesses underestimate their responsibility to each of us and our family. That's why these early cyber awareness programs are an important first step in what will be an extensive road of developing effective cyber education and technologies. It's only through education that we can empower people to protect themselves.

## Education Moves Beyond Awareness

From a policy perspective, cyber awareness campaigns should not be confused with the holistic approaches necessary in an extensive cyber education program. If we truly want a secure future, we must provide education at every level from preschools to senior centers, scouts to boardrooms. Education is our collective social responsibility to help our digital lives tomorrow. The cybersecurity industry, must approach education with the same level of importance as building a defensive solution for the next big enterprise client. Policy must encourage businesses to support cyber education in a more serious manner than what is happening today.

## What should be done over the next decade to better address the challenges; and

### Empower Individuals in Cyberspace

In the next decade, technology must move toward a more reliable, secure and empowering Internet for all of us who use it. With the increasing numbers of devices expected to be connecting to the Internet over the next decade, we will generate more and more data and, with the current technology practices of today, lose greater control over our digital lives. And the artificial intelligence developed as a result of this data sucking, along with decision-making software means who and how we share that data will become more important. For cyber criminals our data will become more valuable. We are at the turning point where technology must advance to provide individuals control—where they first grant permission before providing access to their data—to those tech applications, platforms and software in an easy to understand experience.

### Learn New Life Skills

Our society has become a digital one and we must learn a new set of life skills. Education programs should be put in place that are reminiscent of past programs to fight problems in health, forest fires, crime etc. We need to embark on an all out effort in cybersecurity education. We need K-12 education programs that provide our youth with the tools to be tomorrow's protectors of this new digital world. We should have programs such as public service announcements that (1) teach people how to protect themselves in this new digital world and (2) encourages the young to go into technical fields that will improve cyberspace. This should have a similar feel of urgency as when President Kennedy started us on the path to getting to the moon and back. And then we should provide teachers with technically accurate materials to teach these important lessons.

### Understand Digital Democracy

The Internet genie has been let out of the bottle and there is no going back. We as a society need to move from today's 'Wild West' Internet to one that is based on rules, laws and social etiquette. It is imperative for policymakers to truly understand the cybersecurity issues that are occurring today, and that will get worse tomorrow, as an epidemic. They should begin debates, dialogues and conversation on what it means to be a digital citizen in a democracy in order to better formulate policies that will benefit all of us while allowing technology to advance society.

## Future challenges that may arise and recommended actions that individuals, organizations, and governments can take to best position themselves today to meet those challenges.

Children are becoming increasingly victimized by cyber crimes. While the ubiquity and proliferation of technology has brought us many benefits, sadly we also see its downfalls because too much of today's technology exploits children or takes advantage of parent's naiveté or confusion. They continue to hide behind soft regulations or weak privacy policies and focus on ways to profit from our children's innocence.

Let's just take a quick look at the threat landscape that's emerged for children in only the past few months.

A maker of digital toys for children, said it was hacked putting the personal information of five million people, including children, at risk. The data stolen included the adult's profile information, IP address, mailing addresses, emails as well as the names, photos, gender and birth dates of children. That data could allow someone to link a child to his or her parent and determine that child's physical address.

Another children's media company was hit with a data breach that compromised millions of user accounts, mostly those of children and teens. The information included first and last names, birthdays, genders, email addresses, country of origin, password hint questions and corresponding answers.

Sadly, as adults, we've been accustomed to data breaches exposing our own information or the acceptance of being the victim of digital crimes. But now the game has changed and our children are being targeted. That should make every parent, grandparent, aunt or uncle extremely concerned for all the kids in their lives. Cyber breaches are no longer something to ignore or laugh off.  It's no longer just your future on the line. It's your child's entire digital life.

What we're learning is that apps and software specifically designed to help parents keep their kids safe are, instead, placing those very same children at risk. Earlier this year, a child tracker app, was leaking a huge database with 6.8 million private text messages, 1.8 million images and 1,700 child profiles containing data from their Android and iPhones.

We also saw the Identity Theft Resource Center issue an advisory for parents, instructing them to look out for companies collecting kids' biometric information

for a Child ID Kit that parents can use in case of abduction[5]. On the surface it sounds like these companies have children's safety in mind. Rather we need to be educating parents to ask the right questions before providing their child's data to any company.

You don't have to be a police detective to connect these dots. Our children are at risk, and we as a cybersecurity industry continue to downplay the risk in the public eye. Why? Because it's not good for business. We have to change the public's view of the real risks they face in their daily digital lives. But how can we change their perception of risk, if they have no control, nor responsibility for, their data and ultimately their digital lives?

## Additional Areas of Topics & Challenges

### 1. Emerging technology trends and innovations; the effect these technology trends and innovations will have on the digital economy; and the effect these technology trends and innovations will have on cybersecurity.

In our above comments we discussed the concepts individuals being able to own and control their data. These concepts enable people to share data and to create relationships with others, including businesses and governments, through explicit and transparent actions and agreements. These concepts are becoming known as Self Sovereign identity. This is a trend that is being enabled via new innovations around decentralization, distributed and cryptographic technologies. While these may be new innovations they are actually old concepts. These new technologies are enabling us to better model the natural world for the first time. In the natural world we all know how to establish trust with people we know, typically it starts with reputation. In the natural world we have natural boundaries that allow us to protect property and family. In the natural world we have inalienable rights to life, liberty and the pursuit of happiness. These new technologies are enabling these same rights to enter the cyber world. It is not clear, at this point, what this will look like but it is happening. It is imperative that we begin education programs that tie our natural and digital worlds together.

2. Economic and other incentives for enhancing cybersecurity.

The Internet is still a brave new world that is in need of taming. This is not so different than the rules and laws that have been put in place in the natural world. As our world becomes more and more digital it becomes more and more important to provide infrastructure support for that world.

---

[5] http://www.idtheftcenter.org/Scams/scammy-child-id-kit-companies-coming-to-a-town-near-you.html

In the 1950s—it was determined that we needed a national highway system that lead to major infrastructure investment.

In the 1960s—it was determined that we needed to enter the space race leading to major infrastructure investment.

In the 1970s—it was decided that we needed a resilient network that was resistant to single points of failure. This great infrastructure investment led to the Internet we know today.

We are witnessing tremendous growth that was started by that original investment. However, it is not without problems.

We now need to embark on another great infrastructure effort. This time the effort is less visible – it is in cyberspace. The infrastructure investment needs to come in the form of (1) education of everyone and (2) innovation incentives to build better solutions.

### 3. Government-private sector coordination and cooperation on cybersecurity.

The Cyber Information-Sharing Act (CISA) that coordinates sharing between government and companies in order to identify potential cyber-threats is a start in this effort.

However with CISA, we miss a critical component in sharing—public education

Public health works when the public is involved and motivated to act in its own best interests. And this is why preventing cyber-crimes requires far more than the government and private sector sharing information. It requires involving the public who are at risk, which is to say all of us who use the Internet. We click on malicious links, download infected attachments, or fall victim to online scams, which means we are often the point of entry for these devastating attacks on large organizations.

For government to truly make an impact and succeed it should expand far beyond collaboration of a select group of cyber-insiders. It should promote and support initiatives designed to teach everyone, young and old, about staying healthy in their digital world and learning the warning signs of cyber attacks so we can prevent digital crime rather than focusing on efforts that only examine a disease that's already taken hold.

It is the private sector that also needs to provide the cyber education, combined technology and security that enable all individuals to make safe choices online. This is more than a flashy tagline campaign, it's developing actual technology that helps people safely navigate their digital lives. That's why it is in the best interest of the country for the government to continue to invest in raw research & development in partnership with private industry and academia.

## 4. The role(s) of the government in enhancing cybersecurity for the private sector.

Education is crucial to enhancing cybersecurity in the public. We must remember children are the future workforce who will be defending us on the front lines of cyber attacks. They must learn what cyberspace truly is—a place that's anything but a fairytale, a place with real consequences instead of predictable happy endings, and a place that's based on actual systems and programs developed by real people. The government can work more closely with the private sector cybersecurity companies in order to utilize their professional expertise for the development of curriculum that's based on actual technology, threats and systems.

While technology may seem like magic, it is not. It's science. That's what together, as government and the private sector, can help children understand.

## 5. Performance measures for national-level cybersecurity policies; and related near-term and long-term goals.

Mostly we see the headlines focused on large cyber compromises where adults are victims and those are not showing any signs of slowing down. Then let's look at what's happening to our most vulnerable population, from child abductions and murders that started with unmonitored conversations on social media applications like or the disregard for a child's privacy in the newest wave of summer games apps. When 77 percent of children have downloaded a virus, 63 percent have responded to online scams or even 33 percent have received aggressive sexual solicitation online—one has to wonder if our current technologies and methods of public education are the best we can offer.

When cyber crimes decrease, when identity theft starts to drop, when only a small percentage of children are downloading malware to their devices, when the majority of people surveyed say they have control over their digital lives and when we see a reduction in children receiving unwanted sexual solicitations, can we consider progress is being made.

## 6. Complexity of cybersecurity terminology and potential approaches to resolve, including common lexicons.

Are these words too difficult for you? Basilisk, snuffleupagus, supercalifragilisticexpialidocious, Quidditch, Oompa Loompa. I hope not! They're all part of the magical world of children's literature.

Give many adults these words: Darknet, cipher, binary, encryption, proxy server. All of a sudden, we hear a different story…these words are too hard and complicated. The difference is we approach Dr. Seuss with an open mind, prepared to let our imaginations absorb all sorts of meanings. And we learned that a fizza-ma-wizza-ma-dill is a bird that eats only pine trees and spits out the bark.

Talk to an adult about technology—well, they get a bit freaked out. Why? Because they've already decided the digital world is too difficult to comprehend—no matter how simple the concept. And yet, that same adult is more than happy to help their child figure out how Quidditch is played.

At CynjaTech, we argue that a child's understanding of a darknet is more valuable to their future than learning the diet of an imaginary bird or the rules of a sport played on flying broomsticks. In today's era of digital crime, kids need to know that a darknet is what cyber criminals often use to hide their illegal activities.

That's the conversation we as digital parents and families need to be having today at work and at home. We need to talk about the risks children face when they enter the digital world. When kids are being exploited, harmed or their future digital lives damaged by what is happening online, saying cybersecurity is too difficult of topic for kids to understand is no longer acceptable. It's time to say technology can do better for kids. And then do something about it. That's the progress we need to make.

Technology that combines security, privacy and education together is how we can best address educating the public. Our efforts bring the understanding of public education into the technology we use, rather than just focusing on the next slick tagline which eventually becomes white noise instead of true action. We need to talk about the risks children face when they enter the digital world. When kids are being exploited, harmed or their future digital lives damaged by what is happening online, saying cybersecurity is too difficult of topic to understand is no longer acceptable. It's time to say technology can do better for kids and for all of us. And then do something about it. That's the progress we need to make.

##END##