Sowing the Seeds of U.S. Cyber Talent

Leveraging K-12 Cyber-Education to Develop the Cyber-Workforce and Improve National Security

April 2017

By: James Scott, Senior Fellow, The Institute for Critical Infrastructure Technology

Underwritten by:
Sowing the Seeds of U.S. Cyber Talent
Leveraging K-12 Cyber-Education to Develop the Cyber-Workforce and Improve National Security
April 2017

Authored by: James Scott, Sr. Fellow, ICIT
Upcoming Events

CyberSecureGov
www.cybersecuregov.isc2.org

The Annual ICIT Forum
www.icitforum.org

Visit the ICIT Library to view additional research and publications
https://www.amazon.com/James-Scott/e/B01IPLQKSQ/ref=dp_bypure_cont_pop_ebooks_1
Contents

Introduction ................................................................................................................................................. 4
Why Invest in Information Security Education Initiatives? ........................................................................ 5
How are Stakeholders Promoting K-12 Information Security Education? .............................................. 6
How Might Information Security Education Impact Schools? ................................................................. 7
Cybersecurity and Cyber Safety Education Are Essential ........................................................................ 10
Creating Meaningful Cyber-Security Curriculum Is a Challenge ............................................................. 12
Future Career Paths are Available for STEM and Non-Technical Students ............................................. 14
Why Focus on K-12 to Solve the Cyber-Talent Shortage? ....................................................................... 15
   Students Live on the Internet ................................................................................................................... 15
   Students are the Next Generation of Consumers .................................................................................. 22
Conclusion .................................................................................................................................................. 24
Introduction
K-12 students are “digital natives,” unlike their “digital immigrant” parents. Anyone born after 1994 may not remember a time before the Internet was widely accessible on nearly every device within reach. Some may not even remember a time before touch screens [1]. By 2020, the United States is expected to be deficient by 1.5 million cybersecurity professionals. The digital generation is more tech-savvy and digitally proficient than many are willing to credit. There is a reason that there is a stereotype of a parent or grand-parent asking a teenager to fix their PC or Wi-Fi. If given the opportunity, teenagers already have the capacity to understand malware, attack vectors, Deep Web, and other cybersecurity topics. Consider that the least sophisticated cyber-attackers, script kiddies, are often self-taught teenage hackers. Despite their inexperience, many of these actors manage to launch successful attacks or develop into more sophisticated cyber-criminals and mercenaries. Imagine how the asymmetric threat landscape might shift if these cyber-interested youths could instead be motivated to pursue meaningful careers in Information Security and Information Technology. The younger generations rely on technology, information, and the internet as a necessity to everyday life. K-12 students, who were raised immersed in technology and the Internet, are natural candidates for effectively diminishing the cyber-talent shortage. Further, in a reality where the emergence of automation and artificial intelligence are rendering conventional professions obsolete, motivating younger generations to pursue a field such as cybersecurity, with zero percent unemployment should be obvious. However, simply informing students of the possibility of Information Security professions is insufficient to addressing national needs. Even if the nation filled every open position by 2020, the volume of big data, the dynamicity of the threat landscape, and the perpetual emergence of innovative technologies purposed a skills crisis that cannot be addressed without an immediate investment in K-12 cybersecurity, cyber-hygiene, and digital privacy education initiatives [2]. Even if artificial intelligence alleviates the national burden on cyber-defense, skilled personnel will be necessary to develop, train, and maintain those algorithms and systems.
Figure 1: Why are Deep Web Threat Actors More Willing to Mentor Youths than Schools Are?

Even though many tutoring/mentoring scams persist on Deep Web, it is crazy to think that cyber threat actors might better capitalize on youths’ cybersecurity interest than schools, the public sector, or the private sector. We need a greater investment in Information security education initiatives that identify future cyber-talent and train them to be forces for good.

Why Invest in Information Security Education Initiatives?
Cyber-workforce development and cybersecurity education initiatives have become a priority for the National Governors Association; the departments of Education, Energy, Homeland Security, and Labor; the federal Office of Personnel Management; the National Security Agency; and the National Science Foundation, with NIST’s National Initiative for Cybersecurity Education (NICE) in the federal Department of Commerce playing a coordinating role; President Obama’s national commission on cybersecurity; and President Trump’s emerging cybersecurity reform efforts. That said, privacy advocates contend that civil liberties may suffer if national security agencies alone direct cybersecurity education initiatives [3]. Federal and state agencies are already strained for resources without the additional burden of training the next generation in cybersecurity, cyber-hygiene, cyber safety, and privacy. In order to even offer programs to inspire more students to pursue cyber-workforce careers, these federal and state entities need massive increases in funding. Students who receive government assistance for higher education or after-school programs are more likely to pursue a future Information Security field.

Cybersecurity education can be used to improve national security and to develop a knowledgeable and innovative workforce. Responsible and reputable private sector organizations are vital to more widely promoting a cultural shift in everyday cybersecurity and cyber-hygiene practices and a long-term national security impact. Organizations, which also greatly benefit from the increased talent pool and potential future decrease in breaches, can more easily and more readily provide educators with the training and materials that they need to develop K-12 students into a cyber-workforce.
Investment in education initiatives that promote cybersecurity, cyber-hygiene, and privacy training and awareness are high-yield investments in the future. In an age where typical professions are increasingly being phased out due to automation, it benefits students to pursue careers such as cybersecurity that cannot be automated, that have numerous career paths, and that are critical to national security and long-term national development. Ensured employment, economic stability, and the talent (and tax revenue) of highly skilled cyber-warriors benefit their employer, their city, their state, and the nation. Public and private sector organizations that are perpetually plagued by social engineering attacks, insider threats, and cascading breaches will benefit in the five to ten years immediately following the pervasive and ubiquitous adoption of Information Security education initiatives.

How are Stakeholders Promoting K-12 Information Security Education?
Legislators such as Senator Ed Markey have been actively concerned about the cybersecurity training and awareness of K-12 children, for decades. Bills such as Markey’s Children’s Online Privacy Protection Act (COPPA) regulate sites that target children and improve the overall online experience of the nation’s youth. COPPA requires extra online protections for children under the age of 13 and parental permission for the collection of children’s personal data. COPPA requires websites visited by minors to:

- Have a detailed privacy policy
- Get parental consent
- Inform parents about data collection of Children
- Provide the ability to revoke consent or request data deletion
- Limit the amount of data collected for games or contests
- Protect the confidentiality, security, and integrity of children’s personal information

COPPA actively protects children on the Internet from exploitation by malicious threat actors and nefarious organizations alike. Other legislation such as the Children’s Internet Protection Act (CIPA) requires K-12 schools and libraries that receive federal E-Rate discounts to implement an Internet safety policy that blocks or filters obscene imagery and content that could be inappropriate or harmful to minors. It also requires schools to educate minors on appropriate online behavior, including interactions with others, cyber bullying, etc.

The National Science Foundation works with the Office of Personnel Management to provide “CyberCorps” scholarships to students interested in pursuing Information Security higher education, and it works with the National Security Agency to offer free “GenCyb” summer camps to educators and K-12 students. DHS, NIST, and the office of the Secretary of Defense have developed the NICE Cybersecurity Workforce Framework to provide a detailed catalog of

---

Investment in education initiatives that promote cybersecurity, cyber-hygiene, and privacy training and awareness are high-yield investments in the future. In an age where typical professions are increasingly being phased out due to automation, it benefits students to pursue careers such as cybersecurity that cannot be automated, that have numerous career paths, and that are critical to national security and long-term national development. Ensured employment, economic stability, and the talent (and tax revenue) of highly skilled cyber-warriors benefit their employer, their city, their state, and the nation. Public and private sector organizations that are perpetually plagued by social engineering attacks, insider threats, and cascading breaches will benefit in the five to ten years immediately following the pervasive and ubiquitous adoption of Information Security education initiatives.

How are Stakeholders Promoting K-12 Information Security Education?
Legislators such as Senator Ed Markey have been actively concerned about the cybersecurity training and awareness of K-12 children, for decades. Bills such as Markey’s Children’s Online Privacy Protection Act (COPPA) regulate sites that target children and improve the overall online experience of the nation’s youth. COPPA requires extra online protections for children under the age of 13 and parental permission for the collection of children’s personal data. COPPA requires websites visited by minors to:

- Have a detailed privacy policy
- Get parental consent
- Inform parents about data collection of Children
- Provide the ability to revoke consent or request data deletion
- Limit the amount of data collected for games or contests
- Protect the confidentiality, security, and integrity of children’s personal information

COPPA actively protects children on the Internet from exploitation by malicious threat actors and nefarious organizations alike. Other legislation such as the Children’s Internet Protection Act (CIPA) requires K-12 schools and libraries that receive federal E-Rate discounts to implement an Internet safety policy that blocks or filters obscene imagery and content that could be inappropriate or harmful to minors. It also requires schools to educate minors on appropriate online behavior, including interactions with others, cyber bullying, etc.

The National Science Foundation works with the Office of Personnel Management to provide “CyberCorps” scholarships to students interested in pursuing Information Security higher education, and it works with the National Security Agency to offer free “GenCyb” summer camps to educators and K-12 students. DHS, NIST, and the office of the Secretary of Defense have developed the NICE Cybersecurity Workforce Framework to provide a detailed catalog of
the skills required for a wide range of cybersecurity professions. DHS also offers cybersecurity training courses. The NSA and DHS offer scholarships and grants for graduating high school seniors to pursue higher cybersecurity education at over 200 colleges and universities. Meanwhile, Governors John Hickenlooper of Colorado and Rick Snyder of Michigan have already pushed for state-wide cybersecurity education initiatives, and numerous states are developing career and technical programs that promote pursing higher education in Information Security fields and that enable high school students to earn college credits for cybersecurity coursework from area institutions. Last year, the National Governors Association launched the "Meet the Threat" initiative, which unites educators and employers in efforts to introduce early computer-science and cyber-hygiene education to young children through the use of coding games, competitions, and other mediums [3]. Private sector innovators such as (ISC)^2, Cisco, and others, actively promote education initiatives for use in the education sector and the home.

**How Might Information Security Education Impact Schools?**

![Figure 2: Students are Seeing the Negative Side of Cyber Without the Positive](image)

School databases and digital assets can be remotely targeted and compromised because personnel and students are insufficiently trained in cybersecurity, cyber-hygiene, cyber safety, and privacy.

The Education sector is a growing target for cyber-attackers because its systems are often inadequately secured due to lack of resources, its extensive digital records (medical, attendance, student profile, etc.) are valuable for cyber-criminals, and to an increasing degree, continued operation depends on access to the internet. For instance, one ransomware attack in March 2015 held computer systems belonging to Swedesboro-Woolwich School District for a ransom. The attack prevented students at four elementary schools from taking their scheduled online statewide tests. The hacker compromised the system by utilizing the weak credentials of a third-party
network maintenance vendor. No student data was compromised; however, the attacker did attempt to extort the district for 500 bitcoins or approximately $128,000 at the time. The district did not pay the ransom, but it did suffer a two-week network sanitation and rebuilding period that prevented teachers, administrators, and students from accessing the network.

**Figure 3: Threat Actors are Commissioning False Flag and Cyber-Kinetic Attacks on**

A bomb threat is essentially a Denial of Service (DoS) on a school. It also incites public panic and can lead to numerous detrimental cascading impacts on the community. Threat actors, including fledgling script kiddies, can commission bomb threats on Deep Web or leverage easy to use applications to launch the attacks. Worse, an attacker might be able to commission an actual kinetic attack on a school on select Deep Web markets and forums. Education initiatives are necessary to prepare personnel to work with law enforcement against these emerging threats.

Despite the uptick in cyberattacks, schools have begun adopting BYOD systems and policies, implementing mobile device application management software, digitally storing and classifying data, assigning digital accounts, enforcing credential management, and attempting to deploy multi-factor authentication and software updates and patches. In some instances, K-12 breaches result from unintentional or malicious student activity [7]. For instance, in 2013, a 17-year old student at Sachem School District in Long Island was arrested for allegedly stealing approximately 15,000 student records, including school ID numbers and the names of students on free or reduced lunch programs, and then posting the data on an online forum. In November 2014, the social security numbers of approximately 10,000 of the nearly 24,000 employees (teachers, administrators, etc.) of the Prince George’s County public schools of Maryland, were
exfiltrated in a cyberattack. In June 2015, New Jersey charter school illegally obtained the name, address, phone number, date of birth, and potentially the social security numbers of public school students in a misguided attempt to recruit them via a mailing campaign [7].

Schools depend on the Internet and on “smart” technology to operate. When students, who are used to the digital world, are forced to pay attention to an antiquated projector or the chalk board instead of a smart screen, etc. some students, especially those in over-crowded public districts, lose interest and become disruptive. The inability to access even something as simple as attendance rosters can severely hinder daily administrative operations.

Attackers compromise school systems by exploiting remote access to Internet-facing systems, by infecting a school PC when a teacher or student visits a malicious site or responds to a social engineering lure, or by infecting a BYOD device with malware and laterally compromising the network and as many other devices as possible. Due to a lack of cyber-hygiene, cybersecurity, and cyber safety training, compromising the mobile device of a student or teacher is trivial for an attacker. Consider that many students already visit insecure sites or employ a "free" (often meaning nefarious and subtly malicious) proxy or VPN service to bypass the school filters. Education initiatives can teach K-12 students to act more responsibly and more intelligently on the Internet. They can also raise awareness and concern about emerging threats such as mobile ransomware, commercial spyware, insider threats, etc.

Figure 4: School Personnel Can be Significant Insider Threats

School personnel, or even some students, can prove valuable insider threats for cyber-criminals and other threat actors. Education initiatives can help to raise awareness of the indicators of suspicious behaviors and they can limit the potential of insiders by increasing cyber-security and cyber-hygiene.
Cybersecurity and Cyber Safety Education Are Essential

Students are inseparable from technology and the Internet, and consequently, they are likewise inseparable from the associated perils of online activity. 95% of teenagers aged 12-17 use the Internet daily and 80% use at least one social media platform [4]. Children spend at least 2 hours daily on the Internet. According to the Children’s Internet Usage Study of students in grades 4-8 conducted by the Center for Cyber Safety and Education [5]:

- 70% have a cellphone
- 64% have a tablet
- 48% have a computer in their bedroom
- 87% of students claim to have been taught at least some Internet safety
- Yet:
  - 53% revealed their phone number online
  - 6% revealed their home address
  - 40% digitally connected or chatted with a stranger
  - 11% physically met the stranger
  - 21% spoke on the phone with a stranger
  - 30% texted a stranger
  - 15% tried to meet the stranger

Children are not likely to learn foundational cyber-hygiene or proper online behavior from their parents. Kids, who notoriously avoid parental monitoring of online activities, will not ask their parents when to post online, what sites to use, etc. In many cases, the younger generation may be more privacy conscious and practice better cyber-hygiene than the parent(s) or guardian(s) with which they live.
Figure 5: Children’s PII Are Heavily Exploited by Cyber-Criminals

U.S. Cybersecurity and cyber-hygiene is so inadequate that children’s PII have become a widely available commodity on Deep Web Markets and Forums. Children’s PII, including SSN, are high-utility to cyber-attackers because the information can be exploited for years before the nefarious activity is detected. Further, even after the compromise is discovered, the victim has limited responses since much of the information is characteristic of the identity of the victim.
According to a study conducted by Dr. Richard Power of Carnegie Mellon University’s Cylab, as many as 10% of a sample of 40,000 U.S. children, may have already had their identities or equivalent PII stolen. This rate is 51 times greater than the rate of U.S. adult identity theft [6]. The Cybersecurity and Cyber-hygiene education of current K-12 students is critical to national security and cyber-workforce development; however, it is also vital to the individual protection and potential livelihood of every child whose PII may have already been compromised before they were even old enough to exploit. Realistically, thanks to breaches at OPM, numerous healthcare networks, etc. it is extremely possible that adversaries know more PII fields (full name, date of birth, social security number, etc.) than the children know about themselves. The exfiltrated data is valuable in Deep Web forums and marketplaces, where it is sold as “Fullz" because the relevant PII fields may not be changed throughout the child's lifetime and may be exploitable for years before the victim becomes aware of the exploitation of their identity. Education initiatives can prepare the K-12 students for the eventuality of exploitation, and they can shape them into the next generation of the cyber-workforce through their invested interest and innate digital proficiencies.

**Creating Meaningful Cyber-Security Curriculum Is a Challenge**

The United States cannot continue to be the constant victim of script kiddies, cyber-criminals, hail-Mary threat actors, nation-state sponsored Advanced Persistent Threats (APTs), and other digital adversaries. Our critical infrastructure is buckling under the incessant onslaught of cyber-attacks as citizens suffer the exploitation of their PII and organizations lose Intellectual Property and monetary assets. Cybersecurity, cyber-hygiene, and privacy education efforts should be ubiquitous and pervasive throughout the nation.

Information security cannot be a one-day presentation or a one-week activity. Cybersecurity and digital privacy are year-round concerns [7]. Students need to know how to live and operate responsibly in cyberspace. The adults of the future cannot escape living in the digital world. Every job will require interaction with digital systems. Nearly every activity will require the Internet or an IoT device, and every student needs an education in the foundations of cybersecurity and cyber-hygiene. By teaching students about cybersecurity, cyber-hygiene, and digital privacy, educators can break the self-perpetuating chain of generation after generation of cyber-illiterate users who negligently respond to spear-phishing email after watering-hole lure after social engineering scam. In less than a decade, a meaningful investment in national cybersecurity, cyber-hygiene, and privacy education can curb domestic cyber-crime and stymie foreign cyber-campaigns [3].

At the moment, less than a 25% of U.S. high school seniors have taken a computer science course. Even fewer have received foundational education in technical and highly specialized subjects such as cyber-security. Creating Information Security curricula and programs is
challenging because cyber-security and the technology landscape are perpetually dynamic. Initiatives either have to be so foundational as to not have a significant lasting impact or be so adaptive that they may become too resource intensive for vendors or educators to maintain. Programming languages taught today may not even be used by the time that students graduate. School districts and parents have limited resources, and often suffer from dwindling budgets. Educators are often not proficient enough in cyber-hygiene and cyber-security to teach best practices to the younger generations. Qualified staffing shortages are a major barrier to initiative adoption; especially in low-income and inter-city schools [3]. Federal and state governments and private sector organizations have an enormous opportunity to improve their future cyber-posture by assisting in the development, training, and education of a K-12 cyber-workforce.

For instance, according to the Children’s Internet Usage Study released in April 2016, 87 percent of children in grades four through eight reported that they have learned about safe internet behavior at home or school. At the same time, 29 percent admitted to having used the internet in a way in which their parents would not approve. To close this gap, (ISC)² and their charitable trust, the Center for Cyber Safety and Education, recently partnered with Jim Davis – the creator of Garfield - to release new online and print Garfield materials that tackle different cyber safety issues. Lessons address the dangers of posting online, etiquette, cyberbullying, sharing private information and more.

Lectures, instructional videos, and pamphlets are not effective mechanisms for educating a cyber-workforce. Lasting interest in cybersecurity is best incited through interactive mediums such as hands-on lessons, active discussions, digital mechanisms, and entertaining literature such as comic books and graphic novels, such as those employed in the aforementioned Center for Cyber Safety and Education initiative. Videogames, board games, card games, and role-playing games also drastically enhance the learning experience and improve long-term retention of the educational material.

Only a few reputable stakeholders, such as (ISC)², realize the necessity and added potential of beginning cybersecurity and cyber-hygiene education at an earlier developmental stage (around first or second grade). Most K-12 efforts start teaching cyber safety such as “Stranger Danger”, password security, and responsible information security at the start of middle school (~5th grade). This could be a shortcoming though since younger children are equally if not more dependent on mobile game applications, online television programs, etc. Dan Waddell, (ISC)² Managing Director of the North American Region office, comments, “As we’ve seen with our study data, children are still making alarming choices online. We have chosen to target grades 1-6 with this initial push to give parents and educators more effective tools to teach our youth about the consequences of their online choices. The earlier we start teaching, the more educated they will be on cybersecurity as they enter the workforce later in life. This will have a positive effect on addressing the learning gap and help build the next generation workforce so desperately needed.
to help protect our nation’s critical infrastructure.” Teaching young students of online perils and
of the necessity of parental supervision of their online activities imbeds the necessity of cyber-
hygiene into students when their minds are most susceptible to long-term retention and
developmental manipulation according to cognitive and developmental psychology. If cyber
safety foundations are imbedded into young minds earlier, then by middle school, children can
begin learning preliminary coding, they can learn about more sophisticated online threats such as
malware, and they can develop greater interests in Information Security fields. High school
students can learn “cyber-literacy” and privacy issues within their civics and other courses so
that they understand emerging news stories concerning nation-state threat actors, cyber-
criminals, hail-mary threat actors, etc. Students interested in pursuing Information Security can
take elective courses or participate in after-school programs that experiment with coding,
robotics, foundational penetration testing, and other subjects that would directly contribute to
future cybersecurity careers [3].

Future Career Paths are Available for STEM and Non-Technical Students
Public and private sector organizations, regardless of size or focus, now depend on cyber-
security professionals capable of designing, building, operating, maintaining, and securing
information technology systems and data assets. Within an organization, a negligent janitor can
be as much of an intentional or unintentional insider threat as a software engineer. There is an
increasing need for students to understand the foundations of network security, programing,
cyber-law, digital-ethics, and privacy, before graduating and either pursuing higher education or
entering the workforce [3].

Technical areas of cyber-security require a strong grounding in STEM disciplines such as
Mathematics, Computer Science, and the natural sciences. Cryptography, software development,
network engineering, malware analysis, threat actor profiling, and numerous others depend on an
interest and proficiency in STEM disciplines. However, contrary to popular assumptions, cyber-
security is not entirely about computers. While strong STEM backgrounds are significantly
beneficial, the field as a whole is vast and also contains roles that could be filled by non-STEM
students. In most cases, exposure to the STEM framework and associated thought processes are
as valuable as the information ascertained from each discipline. Much of Information Security
depends on managing people, ensuring policy compliance, assessing risk, interacting with other
disciplines, etc. Some information security professionals do not spend a day of their working
career coding, analyzing malware at a low-level, or doing any form of technical analysis [3].
Why Focus on K-12 to Solve the Cyber-Talent Shortage?

Students Live on the Internet

**Figure 6:** Popular Social Media and Gaming Applications are Easily Exploited
At least 80% of students aged 12-17 use one or more social media platform. Social media sites are designed to encourage the sharing of information and the expansion of networks beyond the familiar contacts of everyday life [4]. These platforms may prove detrimental to young users who are not educated to share as little information as possible online, to adequately secure data, and to only interact with known contacts. Rather than incorporate privacy and security by design, social media sites such as Facebook, Twitter, Instagram, LinkedIn, etc. shift the burden of security and privacy onto the consumer. Most adults have never read the privacy policies of the sites that they use; even if they did, many would fail to understand the intentionally nuanced and
circuitous language employed in the policy. No parent, educator, or social media platform should expect children (who may not even know that privacy policies exist) to read and fully comprehend privacy policies. Nevertheless, social media platforms and other applications that cater towards K-12 demographics continue to shift the burden of user privacy and security onto the consumer. Cyber-security, digital safety, privacy, and cyber-hygiene education initiatives can greatly improve future cyber-posture of the U.S. by teaching young users the best practices on social media platforms such as Instagram, Snapchat, Twitter, and Facebook. Even seemingly trivial lessons such as navigating the maze of user settings in order to harden privacy and security controls significantly reduces the likelihood of the malicious exploitation of young users. That said, teenagers do not need to be spoon-fed how to use social media. The focus of education initiatives may begin with cyber safety at a young age, however, high school students are likely aware of "stranger-danger", "selfie-leakage," etc. Older users are capable and better served by tailoring education towards long-term privacy and security concerns and protections.

Research on the usage and cybersecurity/ cyber-hygiene awareness of minors tends to be conducted by much older adults without considering any meaningful input from educators or the young data subjects. Since these groups have drastically different perspectives on Internet usage, learning methodologies, technological applications, etc. many education initiatives fall flat. Successful education initiatives must be self-aware of the generational and contextual differences within the broader data set. For instance, older teens use social media, gaming applications, and the Internet in general, vastly different than their younger counterparts. Today's youth are in a juxtaposed position. They are chastised for their openness, and the amount of information that they share and they are told that "they don't care about privacy." However, they are also increasingly surveilled by schools, parents, and the government, and they are subject to Internet filters, mobile phone monitoring, location tracking, etc. [1].

The younger generations use the Internet for peer socialization, gaming, relationship-building, etc. Predominantly, though, younger generations use online technology to communicate with people who they already know. Sharing information on social networks and digital clients reinforces bonds of trust within peer groups; it is akin to older generation’s use of a favorite diner or “hip spot” as the point of socialization and community building. Rather than a tangible brick and mortar establishment, the digital generations inhabit neigh-borderless cyber establishments that encompass users from across the entire globe. Physical distances are less of a barrier to communication and socialization, thereby allowing for the possibility of longer-lasting and more convenience based relationships within a broader global context. The obvious risk of the use of these platforms is the possibility of accruing the attention of online predators, cyber-criminals, etc. Students are already taught about unintentionally attracting the attention of predators and other strangers online and about the potential long-term impact that embarrassing posts, photos, and videos can have on future prospects. In reality, students tend to make embarrassing posts out of a misunderstanding of the appropriate use of the platform, a
miscommunication of the social norms and culture, in a state of high emotion (or under the influence of a substance) and when they do not foresee how an audience could perceive their posts or that an audience is more expansive than intended [8]. “Stranger-Danger” messaging, while especially necessary for young users, does little to further impact middle school and high-school students. Meanwhile, education efforts do not provide enough actionable information on avoiding exploitation by threat actors, on limiting malware infection (in fact, most training does not even define malware), or on hardening security and privacy settings and reducing digital footprints.

Contrary to popular assumptions, teenagers do not embrace a fully open, transparent, and public life. Instead, they take proactive steps to restrict their profiles and limit the sharing of identifiable and sensitive information with unknown persons. Based on a survey of 802 teens on issues of their privacy management on social media sites, teens are categorically sharing more personal information about themselves than their predecessors. In 2013, the typical teen had tens or hundreds of Instagram and Twitter followers and hundreds of Facebook friends. Sixty percent of those teenage Facebook users kept their profiles private and were confident in their ability to manage their settings. With built-in tools such as Facebook’s privacy check-up and the emergence of platforms like Snapchat which require confirmation of contact, the rate of young users protecting their privacy by restricting access to their accounts continues to increase. Approximately three-quarters of K-12 social media users periodically purge their networks of barely-known or defunct contacts.
School databases containing grades and other information are popular targets in commissioned cyber-attacks. Though many Deep Web listings targeting said assets are scams intent on exploiting naïve users, others actually deliver on their commission. Education sector systems are compromised via remote access, poor cybersecurity and cyber-hygiene practices of students and personnel, and
Despite students’ desire to restrict access to their accounts and profiles, many still fail to limit the amount of information that they unintentionally share about themselves. This unintended leakage predominantly occurs during the registration of online accounts. Most young users answer account registration information too honestly and provide information even when the field is optional. After the generation of the account, few users remove or restrict visibility of that data. For example, of the 802 teenage Facebook users surveyed in 2013:

- 92% posted their real name;
- 24% posted videos of themselves;
- 91% posted photos of themselves;
- 84% posted interests;
- 82% posted birthdays;
- 62% posted relationship statuses;
- 71% posted their school name;
- 71% posted their hometown/city;
- 53% posted their email address;
- 20% posted their cell phone

High-school students aged 14-17 were 10-20% more likely to post photos, school name, relationship status, cell phone number, and other sensitive information than their younger compatriots [4]. Because students are not traditionally taught the value of aggregated profile information, they fail to secure it according to its value. They do not realize how easily a malicious adversary can exploit that information to inflict physical or digital harm on the individual with only a few more searches on Google or Deep Web. Few teens realize that even a restricted social media account can be laterally exploited or can be used to laterally exploit the associated accounts of friends and family. Education efforts can actively demonstrate to students the destructive power of even a locked social media account if there is significant information leakage. Students can be instructed to either hide sensitive information or to not provide it in the first place. Most accounts can actually be registered with a false location, a Skype or Internet phone number, etc. While doing so may violate some of the terms and conditions of the platform usage, it also better protects these vulnerable user demographics from exploitation.
Limiting the amount of actionable user information also confounds unwarranted demographic and psychographic big data analytics and it mitigates the impacts of unintentional compromise. Only 9% of teens are “very” concerned about third-party access to their data [4]. When they register for online accounts, contests, etc., K-12 users do not consider how their data will be sold, utilized, stored, processed, or transmitted because they have not yet been trained to consider that side of the transaction. Many fail to realize that social media platforms, search engines, and other products and services are free because the economic trade-off is that the vendor aggregates and sells data to numerous third-parties. Data brokers and their clients are proven to be irresponsible data stewards. As a result, many youths’ information has already been exfiltrated by cyber-adversaries. Education efforts can prepare teens for potential future exploitation by teaching them about credit freezes, credit monitoring, account warnings and access restriction, multi-
factor authentication, etc. This foundational education will expose students to the security and privacy thought processes and decision-making skills necessary to pursue an Information Security or Information Technology higher education.

Students are the Next Generation of Consumers

**Figure 8: Poor Cyber-Hygiene Puts Students (and their Parents) at Risk**

The students of today are the consumers and professionals of the future. Without a foundational education in cybersecurity, cyber-hygiene, cyber safety, and privacy, the U.S. will continue to be pummeled by an incessant onslaught of cyberattacks. K-12 students were raised in the Digital Age, they are interested in Information security and technology topics, and many are already more proficient than some of the “professionals” still working in various critical infrastructure sectors. It makes logical sense to leverage their numbers, interest, and potential as the developing U.S. Cyber-
Many cybersecurity and online safety education programs focus too heavily on social media platforms and online interactions. As a result, device security and the fundamentals of cyber-hygiene are pushed to the wayside. Mobile devices such as smart phones, tablets, IoT devices, etc. afford unprecedented real-time access to sensitive personal information. Few users consider the security and privacy implications when using these devices or when downloading applications from marketplaces or the Internet overall. At the times of installation or update, applications request permission to collect and access different information or different hardware and software capabilities. Because their only alternative is not using the application, the vast majority of consumers accept the permissions regardless of the data categories or the amount of access and collection. Privacy studies indicate that even when users are informed of what will be accessed on their device and what information will be collected, the average user does not have an adequate understanding of how the allocated permissions can be used and of the value and utility of the collected data. Most children, teenagers, and adults who download applications are doing so without receiving adequate notice and choice of their privacy decision. Most fail to comprehend that a decision or a transfer of rights even occurs. Exchanges of rights such as these are irresponsible and dangerous. However, they persist because it behooves companies to market their applications to an ignorant population whose data can be surveilled, collected, and marketed. The presentation of simplified privacy implications or a privacy score can drastically alter the user’s decision on whether or not to install or use an application. Companies refuse to implement a privacy metric or transparent data use practices because either their business model relies on the continued exploitation of their user base or they fear potential legal liabilities or market decline associated with an informed user base. What these organizations fail to realize is that by continuing to exploit users, they are perpetuating a nation culture of poor cyber-hygiene and lackluster cybersecurity. Applications, which were likely rushed to market or developed by startups that failed to incorporate security-by-design and privacy-by-design into the production cycle, are frequently and trivially exploited by cyber adversaries. Applications are injected with malware, replaced altogether with malicious imposters, or automatically download poisoned updates onto consumer devices. Apps tend to rely on advertisements for revenue, and those ads can be used to deliver malware or they can lead to watering-hole sites that instantaneously infect the consumer device. Further, the massive treasure troves of consumer information that companies collect for market research, customer transactions, and to sell to other organizations, are valuable targets for cyber-adversaries. Often, the servers containing the aforementioned information are remotely accessible and/or poorly secured with default settings, unhardened defenses, or without layered security proportional to the value of the data [9].

Students can be educated to avoid malicious applications, to protect their mobile devices with layered security, and to harden their security and privacy settings. More importantly, K-12 education initiatives have the power to change our national culture and application dependency by educating emerging consumers of the perils of the marketplace, of the impact of their decisions, and of the ways that they can impose economic disincentives on companies who
employ negligent practices that promote consumer ignorance and that invite cyber-attackers to steal and exploit consumer information.

Conclusion
There will be a cyber-talent shortage of 1.5 million by 2020. Simultaneously, traditional professions will be phased-out in favor of automation and more innovative solutions. Critical infrastructure and the newly-implemented automated systems will be increasingly compromised, and exploited by script kiddies, hacktivists, cyber-criminals, cyber-mercenaries, hail-mary threat actors, cyber-jihadists, and nation-state Advanced Persistent Threats (APTs) and other emerging threat actors. Citizens’ PII, intellectual property, economy, and physical safety will be at the mercy of the horde of cyber-adversaries assailing the degrading U.S. cyber-threat posture. K-12 students are the most prevalent and the most invaluable resource the U.S. can utilize in the development of a skilled and formidable cyber-workforce. The Digital Generations are already more cyber-proficient and tech-savvy than many of their parent and grandparents. However, they need guidance and they need to be informed of the numerous career possibilities in Information Security fields. Education initiatives that inspire developing minds to pursue Information Security through interactive models and engaging mediums are vital to the national security and stability of the United States.
ICIT Contact Information

Phone: 202-600-7250 Ext 101

E-mail: http://icitech.org/contactus/

ICIT Websites & Social Media

www.icitech.org

https://twitter.com/ICITorg

https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit-

https://www.facebook.com/ICITorg
Sources:


