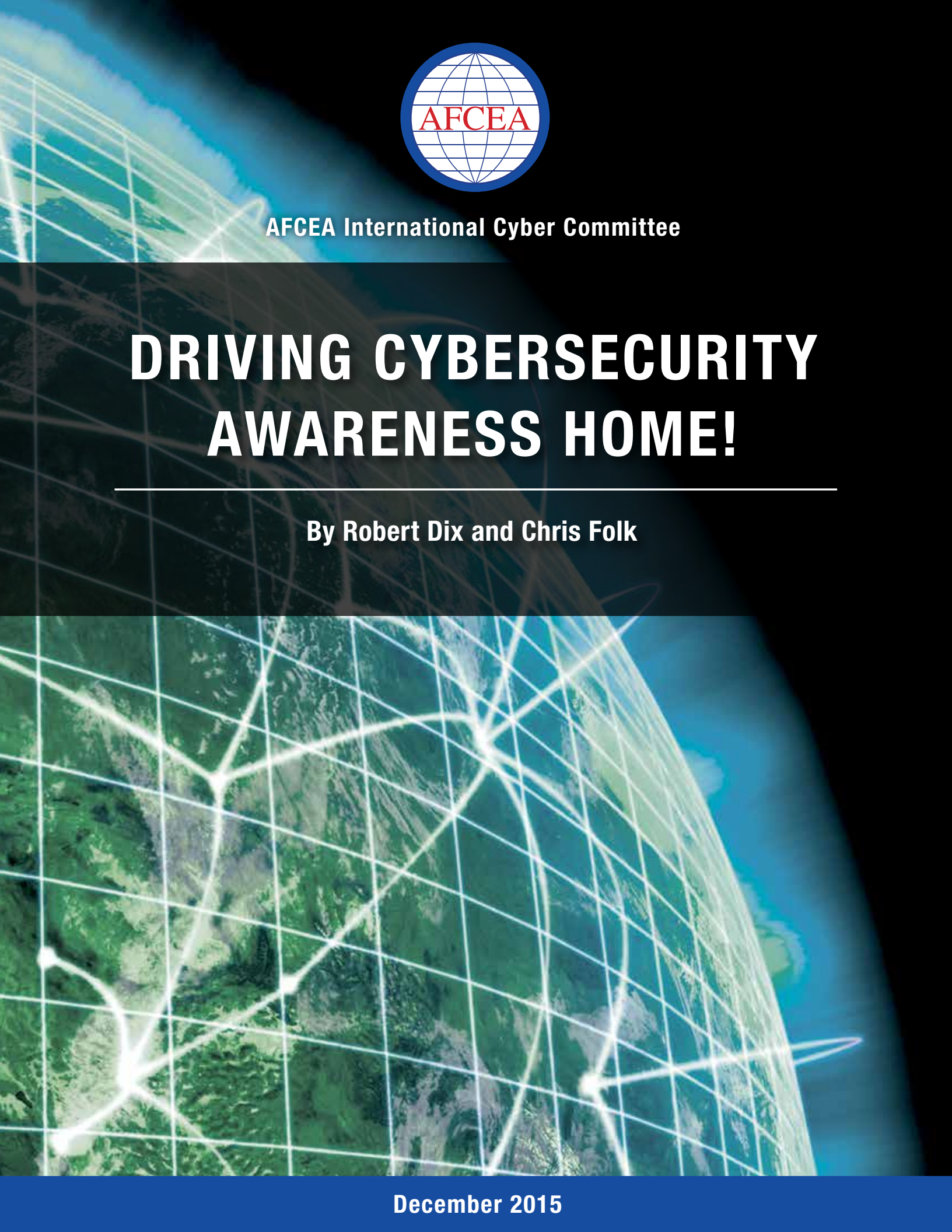


AFCEA International Cyber Committee

DRIVING CYBERSECURITY AWARENESS HOME!

By Robert Dix and Chris Folk

December 2015

EXECUTIVE SUMMARY

In the cyber environment, some realities defy dispute. First, the cybersecurity challenge is pervasive and growing with an ever-evolving range of threats. Second, no one wants to be a victim of cyber crime or a cyber attack, but many people, businesses, and organizations simply do not know how to dissuade cyber intruders.

Accordingly, cybersecurity experts are presented with a great opportunity to come together in a global cyber community—government, private sector, academia, non-profits, and other organizations—to help teach stakeholders of all levels of sophistication about low-cost or no-cost measures to better protect themselves in cyberspace.

Authoritative sources have estimated that approximately 80 percent of exploitable computer vulnerabilities are the direct result of poor or no cyber hygiene. Put simply, users are not taking the basic fundamental steps to raise their cyber protection profile.

This is by no means intended to ignore the 20 percent more dangerous and sophisticated threats, such as advanced persistent threats and destructive malware. However, a comprehensive, sustained national education and awareness campaign that seeks to improve the "80 percent factor" can significantly improve the overall national cyber protection profile.

Such a campaign accomplishes two very important objectives: First, it takes an essential step in raising the bar of cyber protection for everyone by invoking a culture of security and responsibility. Knowledge is a powerful tool, and users do not have to be technology experts to learn better cyber hygiene. Second, as AFCEA has previously documented in two white papers,[1] improved cyber hygiene makes bad guys' efforts more difficult to employ; causes them to have to revise their current tactics, techniques, and procedures; and increases the cost to pursue their craft. All of these serve as an enhanced deterrent to those who today have few barriers to their criminal and illicit behavior.

This paper outlines a blueprint for gathering as a nation to help citizens of all ages and technical sophistication, small businesses, and many other cyber users to learn how to better protect themselves from the wide range of cyber threats. An education and awareness campaign will not be embraced by everyone or touch all users, but the opportunity for creating greater awareness is ripe for collaboration and leadership.

Imagine if every member of Congress, every member of state legislatures across the country, and every local elected official adds a link to their constituent home page that points users to a site where they could learn how to better protect themselves when using their desktop, laptop, tablet, or mobile device. Imagine a national messaging campaign leveraged by the Small Business Administration, the U.S. Department of Education, the U.S. Postal Service, the IRS, and other federal departments and agencies in their communications with citizens and businesses daily. Imagine the powerful opportunity created by a consortium of business and trade associations like the U.S. Chamber of Commerce,[2] National Association of Manufacturers, National Retail Federation, Business Roundtable,[3] and more, leveraging their conduit of communications to members providing cybersecurity tips and pointing to a website with information for all levels of users.

Imagine, for a moment, the ability to reach young people with a comprehensive and sustained program of education and awareness throughout our K–12 and higher education communities that could include a component that also focuses on cyber ethics.

Imagine the entertainment industry joining the effort with a national spokesperson to deliver public service announcements and messaging to help invoke a culture of security and vigilance in cyberspace.

Finally, imagine the impact that American media and social media can have in helping to educate users about where to find information about simple measures that will improve their cyber protection profile.

What's holding us back from coming together as a nation is leadership, coordination, and collaboration to produce the necessary messaging in a comprehensive and sustained manner to fuel a true national education and awareness campaign. Collectively, U.S. agencies have a history of success in such campaigns. For example, just a couple of years ago, they taught folks to cough into their sleeves and wash their hands more often to protect themselves from being infected by the potentially lethal H1N1 virus. Hand sanitization efforts became a regular part of the office, retail, and home landscape. The comprehensive and sustained campaign was effective and likely saved lives.

We can no longer get by thinking, "Cybersecurity is someone else's responsibility," or "A security breach cannot happen to me." Changing behavior, invoking a culture of security, and at least teaching basic hygiene in the cyberspace environment are part of our collective responsibility. The infrastructure already exists to make this happen. In the interest of national and economic security, *let's get to it*.

---

[1] http://www.afcea.org/committees/cyber/documents/EconomicsofCybersecurityPartII-Final4-2-14.pdf; http://www.afcea.org/committees/cyber/documents/CyberEconfinal.pdf

[2] 2015 Cybersecurity Campaign: Improving Today. Protecting Tomorrow.™ https://www.uschamber.com/programs/national-security-emergency-preparedness/2015-cybersecurity-campaign

[3] More Intelligent, More Effective Cybersecurity Protection http://businessroundtable.org/resources/more-intelligent-more-effective-cybersecurity-protection

DRIVING CYBERSECURITY AWARENESS HOME!

BY ROBERT DIX AND CHRIS FOLK

As much as 80 percent of the threats the American public faces today in the cyber ecosystem stem from poor or non-existent computer hygiene.[4] Our adversaries are using the "80 percent issue" to their strategic advantage and systematically degrading our national infrastructure; subverting our economic and military superiority; eroding our confidence in the government to protect and defend; and, ultimately, turning back the clock on American prosperity. The America we live in today allows our adversaries to routinely violate our third amendment rights,[5] pilfer the very essence of our lives, and facilitate the global wholesale exchange of our most intimate personal details. This seems to be all done at will, at little cost, and with no concern of being caught and prosecuted. Alarmingly, this unabated threat—while unintentionally aided by the victims—allows unprecedented access to our systems, data, and lives.

The Challenges the Nation Faces Are a Whole-of-the-Nation Challenge

Cybersecurity is not solely a government problem. All citizens should participate and understand their role. As noted in a January 2014 interview with Peter W. Singer, author of *Cybersecurity and Cyberwar: What Everyone Needs to Know*, " ... the biggest successful attack on the U.S. military, the one that got in their secure networks, all happened because someone picked up a memory stick that they found in a parking lot and plugged it into their computer." Clearly there is an outstanding need for greater awareness, education, and accountability among all citizens.

A 2014 Obama administration report found that so-called phishing attacks—where users are duped into clicking links that open systems to hackers—are the most widely reported cyber incident.

Cyber ecosystem threats today are not limited to nation-state actors with piles of sophisticated weapons and trained national armies. All they need is a computer and the Internet. In addition, the attacks aren't just on government systems—more and more attacks are attempted on corporations, for example, the December 2014 attack on Sony, the September 2014 attack on Home Depot, and the December 2013 attack on Target.

[4] http://www.afcea.org/committees/cyber/documents/CyberEconfinal.pdf.
[5] Alan Butler, *When Cyberweapons End up on Private Networks: Third Amendment Implications for Cybersecurity Policy,* 62 American University Law Review 5 (2013) http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1886&context=aulr

The number of attacks targeted at individuals also is increasing. From 2013 to 2014, social media spam increased 650 percent and 99 percent of malicious URLs with inappropriate content led to malware installation or credential phishing sites.[6] What these significant attacks all have in common are that individual citizens are the target, which begs the question, what can they do to employ basic computer security practices to help them reduce their individual vulnerability and decrease the aggregate vulnerabilities?

Understanding the "80 percent challenge" and the underlying premise behind it—that we can boost our defenses by routinely implementing computer hygiene—can increase our defense game significantly. If we better educate individuals, and if we forge stronger partnerships between citizens and the industry and government sectors, we can raise the cost of attacks to the adversary.[7] ***We can turn the 80 percent problem into the 80 percent solution.***

Gap in Educating the Public

Government agencies, private companies, and law enforcement organizations concentrate on outreach and partnership during work hours; however, an outstanding need to communicate in a unified manner to those who may not be consciously thinking about cybersecurity outside of work hours exists. There ***must*** be a national, easy-to-use program for the average American to reduce the 80 percent low-end threat, thereby raising adversaries' attack costs.

Almost all Americans assume that privacy is protected and systems must be protected or are automatically secure. This mistaken notion and its accompanying doctrine of cyber defense have allowed this view to impede our nation's citizenry to feel a sense of personal responsibility and capability. The combination of these erroneous beliefs and a commonly held view that computers and IT systems are too technical and mysterious abates any personal responsibility on the part of the very users of these systems. As a result, our cyber adversaries exploit the massive unsecured nation and use it to launch sophisticated attacks. Unprotected, unwitting users facilitate our adversaries' ability to use these systems to serve as massive botnet platforms that further exacerbate the attacks.

As citizens use and demand more online capabilities, they enlarge their online presence and become more dependent upon these systems to manage day-to-day transactions safely and securely. Albeit convenient for users, this also permits the exchange of valuable information. Too often, there is an assumption that the information is safe.

There is an extraordinary need to better educate users so they can take personal responsibility for their own safety and security in this space. Currently, there is a gap, primarily because users simply don't understand what the cyber threats are, how their information can be compromised, or what to do. ***We can and must change that.***

[6] *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Friedman and Singer
[7] http://www.afcea.org/committees/cyber/documents/CyberEconfinal.pdf

THE IDEA

Significantly Enhance Our National Campaign of Cyber Education and Awareness

Like the U.S. Stay Safe Online and the UK Get Safe Online cyber initiatives, this proposed nationally led, individually empowered and integrated coordinated program addresses the 80 percent cyber challenge. It raises the nefarious strike costs to our adversaries and enables our cyber defenses to focus valuable time and resources on the remaining challenges facing our cyber defenders. A coordinated and integrated nationally led program would articulate the cybersecurity challenges that leverage existing sets of outreach and communication conduits and mechanisms. The program would combine very easy-to-understand guidelines and employ solutions underpinned by a set of non-product-specific protective measures and best practices. Further, government and private groups who already engage with their customers and constituents would promulgate these solutions to individuals, groups, businesses—especially small- and medium-size—and non-profits alike.

Strategic Drivers

This is essentially a discussion about a cultural change around cybersecurity. Teaching consumers the basics of what they can do, as well as the ramifications of not employing basic computer hygiene, will have cascading effects throughout the IT ecosystem. The end vision is to **empower individuals to protect themselves, practice the basics, AND ask for more.** The individual can go from clicking on anything to pausing and thinking of security first. This, in turn, will foster action, and developers and businesses will bake better security measures into their products. Once the shroud of mystery on "cyber" begins to lift and users have consistent and easy-to-understand information, they will, by human nature, demand products and services that force "security-easy" to be a central feature of their offerings. This cultural shift has to occur, and it must begin today.

Establishment of a national voice on the security of our cyber ecosystem must originate from the top. Currently, there are a number of individual efforts by government agencies, corporations, and other organizations to educate the public about cybersecurity threats. However, with the influx of information and spoofed sites, consumers are overwhelmed with determining what information to heed because it is valid. The Office of the Cybersecurity Coordinator at the White House should be a focal point for a comprehensive, sustained, and coordinated national education and awareness campaign for cybersecurity.

We must not lose sight that markets influence behaviors and vice versa. Empowering the voice of the people to demand change is a powerful tool. If users, consumers, and average citizens are ignorant of the issues and hold onto the belief that cybersecurity is either not their responsibility or extremely technical, change will be elusive. Demystifying this space a bit and fostering a sense of the American can-do attitude along with easy-to-follow advice can change consumers into well-versed and security-conscious technology users.

Integration opportunities abound with and among the numerous federal departments, agencies, and other entities that have an official role or a tacit role in articulating and promulgating cyber defensive messages to their constituencies, customers, or users. The never-ceasing demand and legitimate need for federal departments and agencies to "offer more" and to provide integrative, ubiquitous online services to the American people continues unabated. This extends into every aspect of our lives, which means that those charged with providing services can also provide value. Existing within those relationships are conduits that can be easily leveraged—and at exceptionally low cost—to add value to services by exposing and enhancing security as a duty and right of each citizen. Coordination with the existing capabilities in the government's daily interactions with the public, as well as the myriad other online engagements companies have each day with interested parties, present an already existing venue to reshape and empower the people to regain, or at the very least improve, their own security.

Coupled with and leveraging the enormous communicative capabilities that reside throughout the private sector, academic and nonprofit communities, the prospect of raising awareness across a broad spectrum of the user stakeholder community invites our enthusiasm and our collaboration. What an amazing opportunity to demonstrate true partnership toward a common and national benefit!

Education and broad awareness of what each of us must—***and can***—do to defend ourselves is a key tenant of inverting the onslaught brought upon us by adversaries that rely on our natural reticence to do what we should do.

Together, We Can Stem the Tide and Change the Direction

A one-stop-shop where the public can go for the latest and greatest cybersecurity news and tips as well as obtain more detailed information is needed. Links to organizations and agency websites are just one example of a basic resource. Behind this campaign, a concentrated national outreach effort is required to reiterate the need for individuals to feel empowered, involved, and action-oriented as part of the cyber threat and protection process.

To address this set of challenges, a coordinated national education and awareness campaign is necessary that includes relatable language, easy-open access, coordinated messages, and consistent and broad applicability to all entities in the cyber ecosystem. This multi-step engagement will require dedication and passionate leadership. The first step is critical, and while some basic steps have been taken, the value and usefulness of the current initiatives are questionable.

Fundamental to any national voice is an integrated and coordinated approach to changing the understanding and messaging to energize citizens to accept that this is our call to arms. Famous campaigns that demonstrate the value of a national voice include: Smokey the Bear, Rosie the Riveter, and the personification of Uncle Sam as the United States.

The opportunity exists to launch a similar national campaign for cybersecurity. A symbol and slew of advertising and public service announcements encouraging everyday citizens to be active defenders of their cyber capital to protect themselves and others is sorely needed. Stepping up to a national call to action is part and parcel to the American esprit de corp. Individual accountability is a source of pride and a sense of ownership as American as apple pie. This campaign would play on all those themes and begin that cultural shift in understanding and taking action against this challenge.

Cyber Awareness – Bringing It Back H-O-M-E

Numerous cyber efforts and initiatives are identified and implemented by corporations, agencies, and organizations across America to keep employees safe and informed. But what about the everyday citizen who may not be connected, including retirees, veterans, children, and stay-at-home parents? How do we bring control to what looks like a cyber version of the Wild West? We take it to where the problem manifests, to where the solution rests. We take it to where our strength lies. In short we take it HOME!

PROPOSED CAMPAIGN TO *BRING IT HOME!*

Engagement of Leadership: They say every journey begins with a single step. In this case, the first step is a campaign to sway the administration. This paper, along with leadership from AFCEA, is that first step. Communicating this idea, working to find that integrated and coordinated national approach to cyber education, and increasing awareness to reduce the 80 percent problem is an easy but incredibly powerful platform for the administration.

A simultaneous step is to identify leaders in both chambers of Congress on both sides of the aisle to champion a “call to colleagues.” They must ask their colleagues to make cybersecurity resources a standard link on each of their constituent websites and to support the adoption of this national nonpolitical campaign.

Integrating the Resources: Essential to the long-term success of this effort is the establishment of a place where collective knowledge can be shared and citizens, businesses, and services can convene. This national cybersecurity website, perhaps named Stay Safe Online, would be a singular unique resource that features practical advice about how to protect individuals, computers, and mobile devices. It would include information for businesses about how to battle fraud, identify identity theft, stem the effects of viruses, and combat online threats. In addition, the website should contain guidance on related cyber subjects, such as basic computer hygiene, the elements of a strong password, the importance of backing up data, and the ways to avoid theft or loss of systems, smartphones, and tablets. Every conceivable topic would be included on the site, even safe online shopping, gaming, and dating, as well as how to identify and stop cyber bullying/harassment/stalking.

Fully integrating K–12 and higher education into this program would include teaching cyber ethics, which would add a valuable dimension to this national effort. This one-stop-shop would feature cyber news as well as tips and stories from around the world related to the topic to instruct the students how to protect themselves while online. The website would provide tip sheets, studies, info graphics, quizzes and other resources for audiences. This variety of vehicles would help users digest information in different ways.

The website would be structured to provide cybersecurity resources:

By audience:

- parents (*e.g.,* protecting your children; online monitoring of Web activity; and protecting your aging parents by making them aware of hazards such as phishing attacks)
- businesses both small and large (*e.g.,* best practices in protecting your company's security networks; educating your employees)
- educators
- home users
- children
- government personnel
- owners and operators of critical infrastructure.

By action:

- Instructions about computer protection, safe shopping habits, downloading apps, and the ins and outs of social media will be explained.
- All materials on this website or communicated via other mechanisms would be in easy-to-understand language. This would require establishment and propagation of jargon-free cyber defense terms, ideas, and approaches. One example of the clarity needed is the Stop. Think. Connect. campaign. The site must be written and designed with simple-to-relate-to terms and approaches that average citizens can easily understand and act upon.

The one-stop-shop website also would facilitate the organization of national events, such as National Cybersecurity Awareness Month, and encourage partnerships with law enforcement agencies and other organizations to support their outreach activity, internal awareness and customer online safety. This would include:

- The White House and each state government official and member of Congress would feature links to the Stay Safe Online resources on their website.
- Each federal department and agency would include links to the Stay Safe Online and agency-specific cyber items that are unique to their citizen services. For example, the IRS would have tips about how to protect personal identifiable information and third-party vendor information on its section of the website.

Hence, the website would serve as a mechanism for agencies to share their information, link their websites, showcase their broader efforts, and support cybersecurity.



Establishing the Call to Arms: To attract users to these informational websites, they must be designed in a style similar to the Smoky the Bear, The More You Know, or the H1N1 Awareness national campaigns. Several elements will be required to accomplish this level of notoriety, including:

- One or more national celebrities should be recruited to raise awareness of the information-sharing effort. Someone like Jennifer Lawrence who fits a demographic AND has been the victim of a cyber incident would lend credibility to the campaign.
- Potential partnerships with organizations such as the Cyber Civil Rights Initiative, which is an advocate for ending cyber revenge porn, would bring attention to the new website quickly because of their reach to an established audience and credibility.
- Famous video gamers who may have had their information stolen online would attract the attention of children and their parents then relate to them.
- A commercial to run during the Super Bowl should be created.
- Businesses should be urged to provide basic cybersecurity services and/or products free of charge. Could the government fund this?
- Widespread placement of simple information notices about basic computer hygiene approaches similar to the H1N1 reminders would be a continuous reminder of the importance of protecting computers and personal information.
- "Protect your phone/device from theft" advertisements could be posted in places such as public transportation stations.
- Partnership opportunities and distribution of information by major cellphone providers and Internet of Things device manufacturers should be encouraged.

Government-Centric Initiatives: The federal government is the only place to showcase the commitment and capacity to drive change. To that end, federal departments and agencies must take an active role in beginning to address this 80 percent issue.

- As online citizen services increase, connecting to them should carry a burden of security. Do systems that connect to the U.S. government require certain security standards?
- Any receipt of money from the government should require contingencies for cybersecurity from the recipient.

The HOME Campaign:

H: Hygiene

- Do what you can to keep systems up-to-date.
- Run anti-virus programs and patches.
- Understand what makes a strong password.
- Don't click on suspicious links.
- Stay up-to-date on the latest phishing schemes being reported by news media.

O: Ownership

- Feel empowered and take control.
- Protect your personal information; adversaries are always on the prowl for it.
- When sick, you go to a doctor. Treat your computers and mobile devices the same way. It is up to you to take care of them. Protect them so your devices do not become unwitting accomplices in cyber attacks by helping to spread viruses.

M: Multipliers

Keep in mind that as the capabilities of technologies multiply, so do the avenues for adversaries to attack. For example, over the past five years, many smartphones have become integrated into your life—from tracking your fitness to taking videos to enabling you to communicate with coworkers and friends abroad. The possibilities are truly endless. However, the possibilities for the number of ways you are vulnerable to attack also are truly endless. This environment will only continue to grow as smart technologies continue to be incorporated into our everyday lives.

- Remain aware that a desktop or laptop computer is not the only door into your personal information. Every device you own multiplies the opportunities for adversary mischief and data theft.

E: Ecosystem

Your individual actions are connected to and can impact the entire ecosystem. For example, if you don't keep your computer patches up-to-date, you run the risk of picking up and sending viruses to your loved ones and friends. They, in turn, can forward those viruses on, which leads to a cascading effect of exposed personal and sometimes proprietary information.

- Our nation's leadership, government, and private companies are all responsible for providing tools to keep this ecosystem ***strong and thriving.***
- Consumers should be asking for, no, they should be demanding these tools.



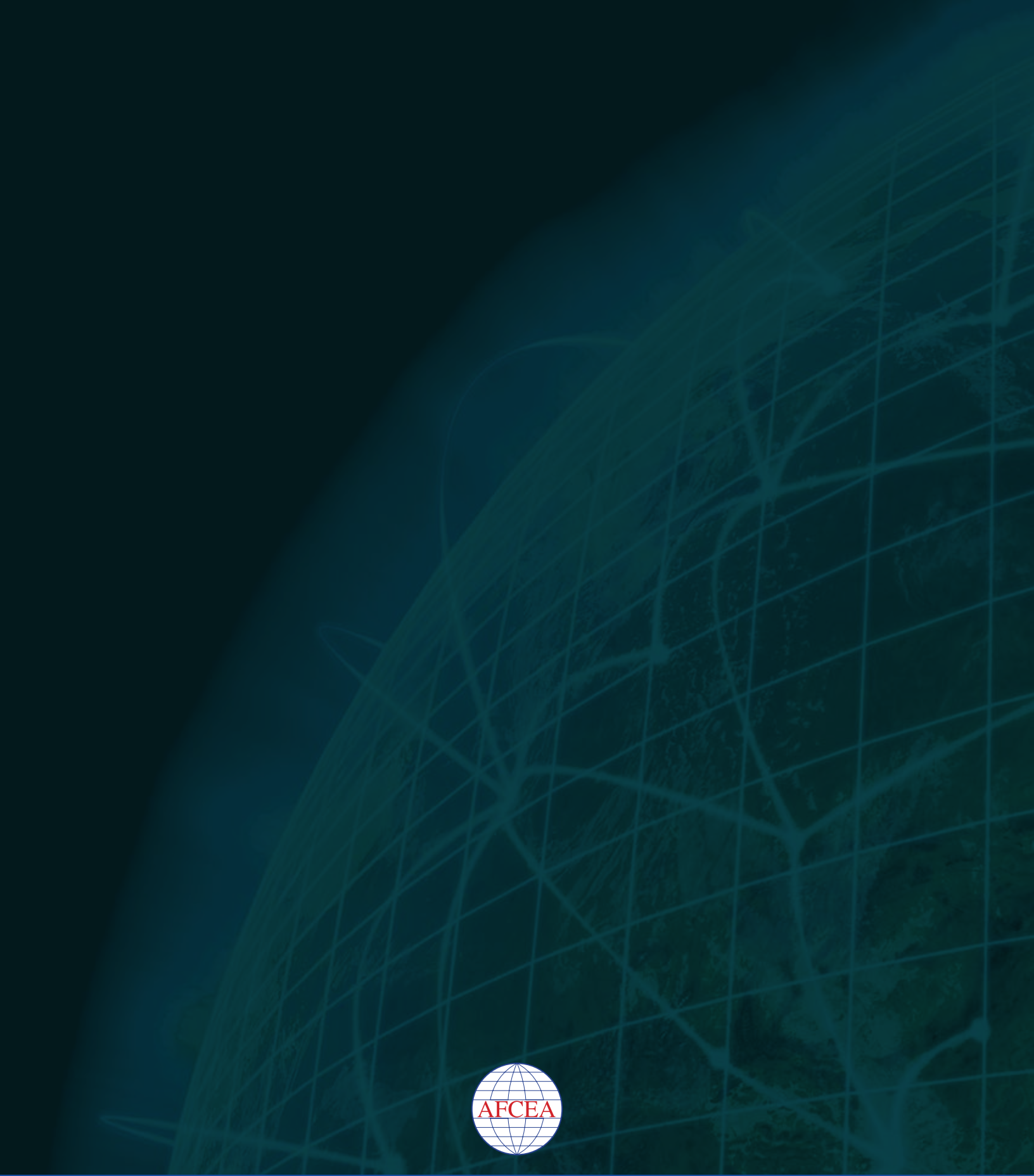
Leadership to Bring This Proposal to the Government's Attention

AFCEA International's Cyber Committee, in partnership with AFCEA leadership, will take the role of assembling this program and making it a specific Standing Subcommittee focus. This subcommittee would play the key role in implementing this effort and coordinating it among stakeholders, including federal sponsorship from both Congress and the executive branch—such as NIST, the Department of Homeland Security, and the Small Business Administration—as well as partners from key private sector companies and trade associations.

The time and attention of the nation on this topic need to be addressed today. Cybersecurity ideas and issues must be demystified. Individual responsibility must be clearly understood, as well as the actions taken by each person to begin addressing what many call the 80 percent problem.

Sophisticated government and industry cyber defenders fight day in and day out with advanced cyber adversaries, when our citizenry does not participate in basic computer hygiene. This leaves the defense of our identities, our personal information, our economy, and our lives at risk to adversaries looking for the easiest way in. Users must understand their role in basic computer hygiene and what they individually can do. Users must ask for more secure products. The government can help facilitate and make sure there are stronger policies and higher standards for security, but all citizens must drive these actions.

This is a way that the Internet generation can fight back; this is a way they MUST engage; and, this is ***the*** way we must signal to our adversaries that we will not go quietly into the cyber ecosystem night. There must be a persistent training environment where all citizens are made aware of the threats; are actively defending their technology; and are aware of what each of them can do in the evolving cyber landscape they live in.



The AFCEA International Cyber Committee White Paper Series

www.afcea.org/committees/cyber