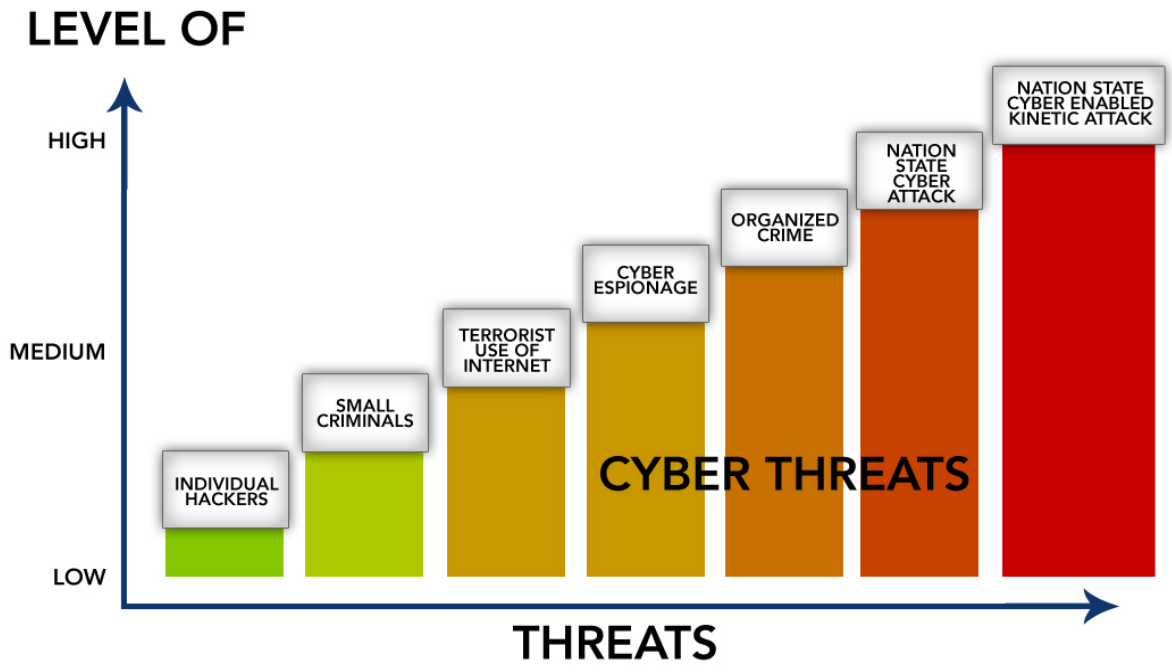
Fostering Cyber Wellness: Engaging the Public in the Battle Against Evolving Online Threats

Published by AVG Technologies

Introduction

Can our national leaders provide us with real cyber security? Will we always be threatened by enemies large and small? Who is going to do the hard work of protecting our networks, our personal information and our communications capabilities? The answer is that a real and lasting solution begins with you and me.

Today the world faces a wide array of cyber threats. The majority of these threats are aimed at the peoples of Western Democracies. The reason for this is simple; we are ripe targets, highly dependent on digital technology for nearly every significant societal interaction. We have come to expect the speed, accuracy, efficiency and ease that a "wired" system of systems brings. The danger we face is that there are many individuals, groups and states that desire to exploit those same systems for their own purposes. Our personal information, commercial intellectual property and infrastructures are at risk, every day. The ubiquitous nature of cyber, the fact that it touches all sectors of commercial, social, and security environments, makes it critical that every citizen understand that cyber security is above all else a personal responsibility.



Too often people assume that the government will provide all the protection they need, that by simply attaching a particular appliance to their computer they will be safe, or most naively, that no one would ever want to "attack" their personal computer. All these presumptions are wrong. Our leaders are struggling to determine how they can effectively

contribute to better security in cyber space, but even the most optimistic will admit that they could never guarantee complete security to all their own systems, and are even further from being able to protect individuals. As yet, no one has developed the "silver bullet" of cyber security. There are many fine software and hardware products that will measurably improve your security, but even the companies that produce them will never claim to have it all. The latter assumption is probably the most dangerous. Thinking that the bad guys would not bother with you is exactly what they are counting on. They do want your personal information, they do want control of your computer, and they will use you and your information to get to those in your personal world, your workplace and possibly our government.

We must take greater responsibility for our own protection, and to protect those with whom we interact online: our friends, family members and co-workers. We can no longer allow a lack of knowledge or desire for pure convenience to leave our cyber front door unlocked and open for cyber enemies to walk through and have the run of the house. We must, as individuals, understand the threat, learn how to combat it and then follow through with our actions. This will require a new degree of education, awareness and commitment.

What it requires is a commitment to cyber wellness.

The Threat Environment

The cyber threats we face today can be grouped into several categories. Any of these threat groups can attack an individual, a business or a country. They will exploit a home computer, a corporate IT system or critical national infrastructure. We are all in danger from these threats.

The lowest level threat is the individual hacker. He operates for his own personal benefit; for pride, self-satisfaction or individual financial gain. At the national level, he constitutes an annoyance, but to the general public, he can wreak havoc. The hacker category also includes small groups who write malware to prove they can or who attack small organizations due to personal or political grievances. Together with the hacker at the low end of the spectrum are small criminal enterprises. These too would be low level annoyances to our federal government, except that their numbers are growing every day. These operate Internet scams, bilking people out of personal information, and may even perpetrate extortion through threats.

Continuing along the spectrum, the medium level threat groupings are of lesser "power" than the high end, but they are ongoing, every day, and this makes them a much larger issue. In the business community, this is the level they fear most, and rightly so. They can, will and most importantly are attacking commercial entities every day. These medium level threats include cyber espionage, terrorist use of the Internet and high level organized crime. All three of these groupings can have extremely detrimental effects on a person, a business, a government or a region.

The high level cyber threats involve the full power of nation-states. These come in two major groups. The first is a full scale nation-state cyber attack. The closest example of this was the assault made on Estonia in 2007. There, the highly developed network of a small country

was temporarily brought to its knees. Portrayed by some as a simple display of public outrage over the moving of a statue, most analysts felt there was more going on and that a government hand was at play. This dispute over the responsibility makes this an imperfect example, but it is a highly troubling harbinger of the future. The other possibility is the cyber enablement of a kinetic attack. So far, we can only look to the 2008 assault on Georgia to study this category. Georgia was not as dependent on the cyber realm as was Estonia, but the cyber assault that preceded the Russian military's ground attack into Ossetia severely hindered Georgia's response by damaging vital public services and communication capabilities. Again, it may be an imperfect example, but these two events at the high end of the Cyber Threat Spectrum give us much to consider.

Everyone must understand the threats we face, or they will not understand the possible consequences if those threats are ignored.

Personal Responsibility and Cyber Wellness

Cyber security should be viewed today in a way similar to how we view public health. Clearly, there is an important role for government at all levels. Government health officials can provide leadership and information that guides the actions of the general population. In many cases, government sets standards and establishes rules, publicizes changes, and provides points of contact through which we as citizens can act. But, ultimately, the most critical links involve the choices we make at the individual and family level about health, exercise, nutrition and the substances we put into our bodies.

Likewise, we need to be mindful of our cyber wellness. There are practices that are wise and effective, and there are others that are counterproductive. In the same way that we teach our children to cough into the crook of their elbow and to frequently wash their hands during flu season, we must now teach them how to avoid becoming victims of cyber illness. Just as we get a flu shot this time of year, we should inoculate our computers against cyber threats. It is only by making good practices a part of daily life that we will overcome the natural tendency to take the easier and, in this case, more dangerous route in their cyber usage.

Today, it is estimated that somewhere between 50 percent and 70 percent of cyber problems could be solved if individuals (children, parents, workers, supervisors, and executives) would follow better cyber wellness practices.

- Protect your computer by applying software patches in a timely manner.
- Recognize (be vigilant for) booby trapped e-mails, Web sites and attachments.
- Apply and keep updated simple software programs for firewalls and security (anti-malware, anti-spyware, spam filters, etc.).
- Properly update and change valid, hard-to-guess passwords
- Avoid unknown thumb drives.

Today we teach everyone to wash their hands after using the bathroom, and after having had contact with other people when there is "something going around." This simple practice radically improves our chances to remain healthy in the physical sense. Likewise, we must begin the systematic process of teaching the basic methods of cyber hygiene to all our citizens. If we can maximize the "protection" provided through these means, we will see the health of our networks improve dramatically, and the effectiveness of all other technical measures improve as well.

Call to Action: A National Cyber Education Campaign

This subject seems to some like a much less important element of cyber security than others. They could not be more wrong. An effective National Cyber Security Education campaign will require strong public-private partnerships and be comprised of at least four vital elements: awareness building, formal education, attraction to the sciences and work place training and compliance. Industry must cross the lines of competition and band together to work with the government to create a unified campaign and message to consumers. The initiative must bring together the large companies like Microsoft and Google with smaller niche companies such as AVG Technologies to provide a focused, product agnostic message that provides consumers with clarity and a call to action. Technology companies must forge a strong coalition that is dedicated to moving their consumer awareness campaigns away from efforts to enhance their images to ones that provide citizens with objective and actionable advice. The initiative should be led by government and supported by industry partners. These efforts would raise the level of understanding and acceptance of personal responsibility and give the tools through which citizens can exercise it. All are vitally needed to ensure a transformational behavior shift that "sticks" with the American public.

The effort requires sustained messaging along the lines of the highly successful "Smokey the Bear" national public awareness campaign that blankets the country. It must reach to every level of our society and get across the message that cyber security is important to every citizen and that every citizen has an obligation and role to be a good steward of the Internet. It has to help citizens more fully understand that everyone can be, and in fact is, affected by cyber threats. It must promote the concept that by awareness, proper procedures and active sharing of information, we can achieve a high degree of security. We must create a culture where private citizens understand that they are an integral part of our national strategy to secure our cyber borders.

This cultural ethic must become a mandated part of the formal education curriculum beginning at the earliest academic levels (today kindergarteners use computers) and be seen on every street corner and during primetime television hours. Many private companies and foundations have outstanding work on this front, but their reach is limited. Some federal departments now have kids' campaigns, but none are anywhere near the level of comprehensiveness needed. An effort needs to be made to coalesce the best of these campaigns and spearhead the resources into an integrated and strategic campaign that harnesses the power of government Web sites and is flanked by a strong national advertising and PSA campaign. The Ad Council should be enlisted to devise and champion the effort in concert with industry leaders, celebrities and national leaders. The Ad Council is famous for successful campaigns in

partnership with government that are aimed at changing behavior – "don't start forest fires," "wear your safety belt," "buzzed driving is drunk driving" – personal responsibility in cyber hygiene needs to be broadly messaged and adopted. If we can make Americans aware of the problem and their critical role in the solution, we will have made huge strides. The initial step in taking responsibility is recognizing the problem and acknowledging our role in addressing it.

Awareness is the first step. But Cyber Citizenship should begin at the earliest stages of the formal education process. So the next part of this campaign is to actively train our young citizens in cyber security. They are masters of using the newest technologies, but they do not necessarily understand how these technologies work or their vulnerabilities. They must understand the magnitude of the risks they create by not using safe Internet practices through normal channels in their schools. Meanwhile, technical and technology courses should be expanded in curriculums at all levels of our educational system--and the earlier the better.

To date, technology education has been largely focused on driving children to careers in math, science, and engineering and not augmented with efforts to provide them with core skills to ensure they are safe online. Before children are exposed to the power of the Internet as a learning resource, they should be made to understand in age appropriate messages its risks. We need to uniformly take our "Stranger Danger" programs to the next level. Just as one would never consider letting a young child walk the streets and play in the parks without first teaching them basic personal safety tactics, we must make similar, age appropriate efforts to make them not just street smart but cyber-street smart as well.

Even if children choose not to pursue careers in the math, science and engineering fields, they need to be educated on the means through which all commerce and communication is now occurring. Additionally, this would contribute to the number of young people who would steer toward careers in technical fields by allowing some to realize that these fields are more interesting and exciting than they might have otherwise thought. No field of endeavor today is untouched by technology, and the ubiquitous nature of cyber communications is only going to intensify. Even those in completely non-technical fields will need this education.

The third leg of the campaign should promote incentives to attract more people into the math, science and engineering fields. Targeted scholarships for these programs at the college level are a good start and should be started immediately. Additionally, there must be programs at the high school level that are attractive to teens and provide productive outlets for the many that possess incredibly strong technology skills. By engaging them in the solution, we minimize their participation in activities that are actually detrimental to the broader security of the Internet. These could be predicated on future college scholarships, incentive funding, potential job opportunities, and other methods to draw students. Particularly in public schools, great efforts must be taken to move away from general programs to targeted ones that steer toward the sciences. We must more effectively harness the "CSI phenomenon" and engage our teens in being a part of solving Internet crime as opposed to creating online nuisances. Not everyone will be a software engineer, but the more people in our population who are exposed to the concepts by which technology works, the more protected we will be.

Finally, there is a need for standardized, baseline training and education for employees in companies of all sizes and across all sectors. This must go beyond a "check the block" approach. Today's global economy requires a work force (public and private sector) that not only understands technology and the threats that exist, but who see themselves as key layers in protecting the cyber realm. This program would include workers on all levels, both in tech and non-tech positions, and those in white-collar and blue collar jobs. It should address issues that workers need to know to properly perform their work, but also what they need to know to protect their personal/individual systems in the cyber realm. This is a key aspect, as a large segment of the present work force will not have been reared on the campaign as their children will be. These cyber citizens must be reached at work.

In the workplace

In our highly interconnected world, the people with whom we work or go to school are not isolated from us. What they do can have an effect on our security. We are infinitely more vulnerable when coworkers are poorly trained or unaware of the possible effects of their actions. We often speak of "insider threats," and these are an enormous part of cyber problems we face. Actions by humans working for us; be they simple mistakes or malicious acts, account for the vast majority of cyber breaches. We can have the best technological security systems available, but if we fail to recognize that a fellow worker is not adhering to cyber wellness practices, or is behaving in a peculiar or suspicious manner, our organization can be penetrated by a competitor or enemy. Additionally, in an age when a huge number of workers operate remotely, travel a great deal or work from home, the failure of one fellow worker in cyber wellness can effect not only your work network, but might be harmful to your personal one as well. Everyone's personal responsibility extends to those around them, and we should emphasize that aspect as well.

Leadership

In the past, many in positions of agency or business leadership have entrusted their organization's cyber practices and infrastructure to their technology, security or legal practice subordinates. This has been understandably true among senior leaders with little cyber training or familiarity with technology. However, today's environment compels our leaders to learn the technology, to learn the threats, and to more effectively engage their technical staff in the development of solutions. They must make cyber security a priority for their organizations by fostering a spirit of accountability at all levels. They must mandate checks and inspections to ensure cyber citizenship at the enterprise level, and must oversee exercises to test the status and resilience of the organization. Traditionally, these activities have been viewed strictly as expenses. However, forward-leaning executives are increasingly recognizing them, instead, as investments in protecting their organization's reputation, assets and personnel—not to mention mitigating liability concerns.

Policy efforts to create a climate that enables, encourages and rewards consumers for taking the right actions should be pursued aggressively. Business and government should work together to create produce agnostic, government-sanctioned Web sites where consumers can get trusted information on available tools. Tax incentives for both consumers and businesses should

be offered to those who are doing their part and making investments in the myriad of powerful Internet security tools in the market. Finally, the power of the e-government tools must be used as means to get people to think about Internet security and to take action

Information Sharing

Information sharing is critical to properly addressing cyber security. As the Center for Disease Control (CDC) must have open information sharing if it is to help us fight pandemics, cyber security must have the same level of openness, or security and resilience efforts will fail.

Today we have two main organizational impediments to open information sharing in the cyber security arena. On the government-to-private sector side, the problem is government reluctance to share all the threat information it has because they want to protect their intelligence sources and methods. On the private sector-to-government side, there are actually two problem areas. The first is a fear that proprietary industrial information will be revealed. The second area is the fear that the government might use the information given by a private company, and the company would be held liable for any damage done or for any breach of the law. All of these concerns are legitimate and understandable; they are also problems that are clearly surmountable.

Programs have been undertaken by agencies (such as the Department of Homeland Security) to solve these problems; however, participation has not been widespread. Re-engagement between government, the private sector and interested third parties should take place to determine the effectiveness of current programs or to determine a speedy and more productive way forward.

In the cyber realm, the government must do the hard work of developing trusted partners with whom they can share the most sensitive information. This will be a cultural change but one that must occur. Additionally, a method of redaction must be developed in the short term that allows the maximum amount of sharing and the most useful format for the information, while still protecting sources and methods. It is not enough to say it is "too hard" and do nothing. We must find a way. This applies to the personal side as well. The government must be able to share information with the population in general, who has the personal responsibility to use it correctly.

In the other direction, the government needs to help the private sector to develop a way to pass on information of attacks, penetrations, and even successful defense techniques while protecting the industry equivalent of sources and methods. There must be sensitivity toward protecting proprietary information that raises the comfort level of the corporate leadership. The next step would be the development of a real liability protection for companies trying to assist the government. There must be a legislatively founded exemption program that specifically protects these companies. This needs to be further backed up with a real insurance protection program that would indemnify any firms that might fall through a crack in the legislative exemptions. Again, individuals need to be enlisted in this effort. They need to feel comfortable in reporting cyber incidents quickly and accurately. This would require developing a central clearing house for individual reports.

Civil Liberties

Cyber wellness starts with a good citizen ethic. And good citizens are respected by their governments. Therefore, the protection of civil liberties must remain a priority. Privacy and security are not mutually exclusive. The American people have always demanded a level of privacy from their government. Regardless of intent, some may see any security action as at least a great imposition, if not an outright threat. To most Americans (and world citizens), the freedom and anonymity of the Internet is a right; one which they will not surrender lightly. If any strategy fails to adequately address this concern, it will fail. It is not acceptable to cry "National Security" and be seen as dismantling the freedoms upon which our country was founded, and which make it worth defending. Protection of civil liberties must be built in to the strategy for awareness and education from its inception.

Civil rights organizations, privacy advocates and individuals alike must be enlisted along with industry leaders to aid in drafting of the educational materials in order to adequately defend both our rights and our security. Civil liberties activists must truly understand how much would be lost if we take a passive stand and do not aggressively move to protect our security. A collaborative give-and-take will improve the process and give it greater credibility.

The Government must publish realistic threat reporting so that the American people can make valid decisions as to how much of their freedoms they are comfortably willing to effect in order to have security. Protection of privacy and civil liberties needs to be seen as the cornerstone of any cyber security effort, or it will eventually be rejected by the American People and deemed a failure. This balance can be achieved by adequate and ongoing public engagement.

Conclusion

The issue of cyber security is too critical to leave the individual citizen on the sidelines. Our world is a complex and interdependent network of infrastructures that leaves no one immune to cyber threats. But regardless of how effective our technological solutions become, without a robust citizen education and empowerment campaign, they will ultimately fail. The true key to national cyber security lies with the people. We are convinced that given the proper education and training opportunities, they will step forward and accept the challenge to become true cyber citizens. The American people will make cyber security a personal responsibility and will do what it takes to protect themselves, their families, their coworkers and their nation.