Increasing Cyberspace Awareness

Larry K. McKee, Jr., NSCI
November 26, 2010

National Security Cyberspace Institute, Inc. (NSCI)

Through the combination of research and education, NSCI supports public and private clients aiming to increase cyberspace awareness, interest, knowledge, and/or capabilities. NSCI is committed to helping increase security in cyberspace whenever and wherever possible. NSCI publishes a bi-weekly newsletter (*CyberPro*, details below), has published numerous whitepapers on various cyberspace topics, maintains an online cyber reference library, and has established an email distribution list for sharing cyber-related resumes to interested parties. NSCI is a small, veteran-owned business headquartered in Virginia.

Executive Summary

Cybercrime is here to stay. It would be unrealistic to think in terms of totally eliminating the threats and vulnerabilities. We must find ways to mitigate the risk, and this requires organizational and individual cybersecurity awareness alike. Government, industry, academia, and casual users must be equipped with cyberspace threat and vulnerability information so they can keep themselves, their organizations, and their families safe and secure on the Internet. This is especially critical in areas including national security, personal safety and comfort, commerce and business.

Increasing cybersecurity awareness for organizations and individuals will be difficult at a time when cyber threats are increasing while funding and focus for security programs are failing to keep pace. While government organizations, such as the National Security Agency and U.S. Cyber Command, and many large businesses appear to have the resources necessary to ensure at least an adequate cybersecurity awareness, those in the "have not" category include individual users, small- and medium-size businesses, educational institutions, non-profits, and others. Government can help by ensuring all organizations and individuals have simple, easy access to at least a minimum level of cyberspace awareness.

At a minimum, cyberspace awareness should increase knowledge of cyber threats, vulnerabilities, and solutions to minimize risks. This will help prevent organizations and individuals from making decisions and mistakes that could expose data, money, systems and networks to exploitation by cyber criminals. The additional increased awareness will pay benefits in terms of reducing the time spent responding to attacks, the disruption to business operations, revenue loss, and destruction of property and equipment. In addition, with required U.S. cyberspace worker shortfall estimates ranging from a few hundred to thousands, it should be noted that increasing awareness is likely to raise the profile of the profession and attract the interest of talented youth.

Introduction

During his historic speech on cybersecurity in May 2009, President Barack Obama called for a national public awareness and education campaign as one of 10 short-term action items. There is little debate "cyber terrorism"[1] is on the rise and neither national governments nor the general public are fully prepared to deal with the threat. Cyber attacks are viewed by many as a major threat to national security. President Obama's intent is clear: improve cyberspace for everyone — individuals, private sector and government — who conducts business online. Increasing cybersecurity awareness for organizations of all kinds — government, businesses, nonprofits — and computer users of all ages will help to improve cyber hygiene and raise the bar of protection for all of us.

> ***"It is our shared responsibility to create a safe, secure and resilient cyber environment."***
> ***Howard Schmidt, White House Cybersecurity Coordinator***

There are daily attacks on networks, computers, mobile devices, web sites (including social networking sites), and even personal/private information. The threat includes everything from phishing emails, spoofed websites, unpatched or unprotected PCs, open wireless connections, not shredding data, and overall lack of attention to personal security. Typical goals of these cyber criminals and/or attackers

[1] We use the term "cyber terrorism" generically to include cyber espionage, crime, attack, and terrorism.

include theft of intellectual property, confiscating online bank accounts, distributing viruses and other malware, posting confidential business information on the Internet, and disrupting a company's infrastructure. Risks are compounded by the increasing popularity of new technologies such as mobile banking and social networking. The threat to and within cyberspace is constantly evolving.

Our collective lack of awareness allows this criminal activity to flourish. While President Obama's statement has started us down a path to increase safety and security online, developing and maintaining an awareness of the vulnerabilities, threats, risks, and solutions in cyberspace remains difficult. If we hope to defend our country in the cyber domain, our government must continue to foster awareness programs that inform organizations and individual about cyberspace. We must keep ideas fresh and cyberspace users aware of and knowledgeable in vulnerabilities, potential threats, and mitigation of risk.

"We all share a responsibility to prevent cyber attacks and increase our nation's resilience to cyber threats."
Janet Napolitano, Secretary of Department of Homeland Security

It has often been said that no one agency within the federal government can do it alone. In fact, the federal government as a whole cannot do it by itself. Given institutions and individuals are at increased risk of having their information compromised by hackers, malicious activity, or mistakes, cybersecurity must be viewed as a shared responsibility among Internet users, academia, industry and the government. It will require a collaborative effort from all stakeholders to counter the ever evolving risks of operating securely in cyberspace. The first step in facilitating this collaboration is increased awareness by all interested parties.

Awareness, Education, and Training

We would be remiss if we did not spend at least a few minutes explaining our view of awareness, education, and training. While all three are important to achieving the goal of a safe and secure cyberspace, we believe awareness shares the most commonality among cyberspace users. Because a lack of awareness on the part of victims is instrumental in so many successful cyber crimes, awareness would seem to be a logical starting point and building block in any effort to enhance security. Further, it is likely that increased awareness will lead to an increased interest in education and training for those wishing to further their knowledge of cyberspace. Although it is impractical to provide advanced cybersecurity education and training to the entire populace, we should certainly be able to enhance our security through more aggressive efforts aimed at increasing awareness.

The best, most affordable, most effective defense starts with an awareness of cyber threats, vulnerabilities, and risks. Raising awareness will enable organizations and individuals to be active participants in protecting themselves and will further generate additional interest in cybersecurity.

Organizational (government, industry, academia) and Individual Awareness

The discussion of awareness in this paper refers to awareness of a generic nature. While there is a need for specific, high-level cyberspace situational awareness such as who is on the network, why they are on the network, and what they are doing on the network,that is not the type of awareness we are addressing here. We are more focused on the kind of cybersecurity information that is useful and actionable to a larger audience — information that is generally of benefit to individual users, government, and law enforcement, as well as energy, medical, financial, retail, educational and other organizations.

Few would argue that both organizations and individuals need to ensure their networks and computers are protected and secure. Improving organization and individual cybersecurity awareness must be a central objective.

"We need to continue to advance a national education and awareness effort to inform all user communities of how to better protect their IT assets."
Bob Dix, Vice President of Government Affairs and Critical Infrastructure Protection, Juniper Networks

NSCI National Security Cyberspace Institute

Increasing Cyberspace Awareness

Larry K. McKee, Jr., NSCI
November 26, 2010

All organizations depend on a secure cyberspace to conduct daily transactions, both internally and externally with "customers." In many cases, the need for a general awareness of cyber threats, vulnerabilities, risks, and solutions is common across these organizations, both large and small. However, time, money, and personnel constraints often serve as impediments to enabling this commonality. Staffing a large security and/or network department is simply not realistic for many small businesses, nonprofit organizations, and others -- although the need for security is just as important.

While numerous organizations have made progress in maintaining a minimum level of cybersecurity awareness, individuals largely remain the weak link and frequently offer the path of least resistance for cyber criminals. The same people who use computers at work also use them to shop, bank, or socialize from home. We increasingly rely on the internet for everyday tasks such as banking, shopping, education, and communication. And while people are only just beginning to realize how the Internet can enhance their lives, sadly, many are blissfully unaware of the potential dangers. Cybersecurity risks are often simply not as obvious to non-technical staff or members of the general public.

Numerous malicious programs are designed to steal information from users without their knowledge. For example, hackers might log keystrokes as a user enters information into online forms, or remotely harvest data stored locally on a computer. Other examples of internet-threat ignorance include parents who are often ill-equipped in new technologies to educate their children about online safety, and young "digital natives" who are skilled at using technologies but frequently know little about potential online threats. These are but a few of the numerous examples where increased and continued user awareness could reap huge benefits.

Members of the general public frequently "don't know what they don't know" and are unaware they are being targeted. Too many people are making unsafe decisions online not because the information, technologies and techniques are not available, but because they simply don't know any better. Users must understand that if they have access to information, they may also inadvertently allow unauthorized access to that information. A more proactive approach to user awareness must make it easier for the average home user to know about threats, vulnerabilities, and solutions. They should not have to be an expert on cybersecurity or the latest phishing threat.

Individuals require awareness of the security threats posed by computers, the internet, and emerging technology and the things they can and should do to protect their part of cyberspace. They cannot simply believe that someone else is protecting their data. With greater awareness, users can start to link uninformed behavior to their risk of becoming victims. In turn, we can expect a new alertness when dealing with e-mails, attachments, and obscure web sites, more caution with passwords and when using social networks, and watchfulness regarding mobile devices such as laptops, cell phones, and USB sticks. A security-savvy user is more likely to become involved and active in securing cyberspace. If the lack of user awareness is left to persist, public ignorance will continue to be the weakest link in cyberspace security.

Changing threat...continuing awareness

> ***"As we look at the evolution of risky domains and websites over multiple years, we can't avoid the conclusion that the risk keeps increasing in both volume and sophistication."***
> ***David Marcus, Director of Security Research and Communications, McAfee Labs***

Change in cyberspace has accelerated and shows no signs of slowing down. Organizations and individuals will need to stay abreast of this continued pace of change if they are to remain ahead of the dangers. We must view awareness as an ongoing activity - not a single event - to keep up with the evolving threats. No matter how much awareness and security savvy we have today, we must remember that malware purveyors are constantly working to adapt their product to improve upon bogus e-mails, spoofed websites and other traps to make them look more genuine. It seems new uses for the Internet are invented every day and it's not always clear whether new activity is harmful or benign. Common sense may not always result in the awareness that taking a seemingly benign action, such as clicking on a link, could be harmful.

"It's so important to keep talking to people about the old threats, the new threats – on a recurring basis."
Anne Wallace, President, Identity Theft Assistance Center

Increasing Cyberspace Awareness

Larry K. McKee, Jr., NSCI
November 26, 2010

CyberPro Background

CyberPro began in 2008 as an effort by National Security Cyberspace Institute, Inc. (NSCI) to increase the awareness of cybersecurity issues. We envisioned it as a platform to simplify and improve access to cybersecurity information for those in government at the federal, state, and local levels, as well as the private sector, non-profit organizations, academia, and the international community. In short, our goal was to make cybersecurity accessible, participatory, and popular. As cyberspace threats, vulnerabilities, and solutions continued to evolve, so did our content and targeted audience. As an example, the importance of casual users and students to online security necessitates a level of cybersecurity awareness comparable to that required by organizations. In addition, the challenge is no longer in finding information; it is sorting through and finding the time to read it

After over 30 months and 60+ editions, we have been partially successful. Our distribution has ranged from 3,000 to 6,000 recipients, including congressional members and their staffs, several Fortune 500 businesses, research organizations, the departments of Defense, Homeland Security, and Education, and other government departments and agencies. However, the time and effort involved in sifting through RSS feeds, web sites, trade journals and other sources for relevant articles, events, and training courses; reading and summarizing the articles; interviewing senior leaders; working with contributors regarding feature articles; maintaining distribution; and actually putting the publication together have necessitated a subscription price that is just not within the reach of a larger populace. As a result, significant numbers of academia, non-profits, small business, government departments and offices, and individual users remain missing from our subscriber base – this in spite of their considerable interest and inquiry into the publication. Simply stated, we have been unable to reach the masses we envisioned.

In an effort to further raise awareness about the importance of cybersecurity and help ensure a safe a secure Internet, we are seeking your support to increase our subscriber base. *CyberPro* is a proven product that has been successful in raising the cybersecurity awareness of numerous government and business leaders. We believe additional access to this information by schools, colleges and universities, government, law enforcement, consumers, businesses of all sizes, and others can be central to boosting cyberspace awareness and the overall effort to improve cybersecurity nationwide.

Thank you for considering partnering with us to increase the availability of this resource. With your help, we will expand *CyberPro*'s reach, contributing to a safer cyberspace, further publicizing cybersecurity, and increasing cybersecurity interest. We look forward to hearing from and working with you.

CyberPro

CyberPro is a bi-weekly publication aimed at increasing awareness of cybersecurity issues and growing interest in becoming part of a much-needed cyber workforce. It is intended to increase the awareness of organizations and individuals who, despite having a need or desire to establish and maintain cybersecurity awareness, do not have the time and/or resources to dig through the numerous articles and web sites available. *CyberPro* contais a short summary of open-source news articles with a link to the original article. In addition, editions contain an interview with a senior cyberspace leader, a capability spotlight regarding specific cybersecurity products, or a best practices list specific to a cybersecurity challenge. Articles are included independent of policy position, politics, or other potential biases. Below are the major CyberPro sections and a description of the content typically found in each section.

Cyberspace - Big Picture

This section is usually limited to less than 10 summarized articles. The summaries included here are strategic in nature - often dealing with cyber policy, doctrine, senior official statements, etc.

Cyberspace - U.S. Government

Included here are items related to the White House and federal/national organizations.

Increasing Cyberspace Awareness

Larry K. McKee, Jr., NSCI
November 26, 2010

Cyberspace - Department of Defense (DoD)

This section is specific to DoD cyber-related items.

Cyberspace - International

A look at cyber news from around the world.

Cyberspace - Research

The overall purpose of cyberspace research is to minimize the risk to society. Cybersecurity researchers are trying to develop new technologies and increase education efforts. In this section, we provide information on research efforts such as cyberspace trends, information assurance, cyber operations, computer science and software engineering, human vulnerabilities, computing devices, and others.

Cyberspace - Hacks and Attacks

The "Hacks and Attacks" section helps ensure awareness of threats such as malware, botnets, identity theft, network viruses, loss of sensitive information, security breaches, and other malicious activity that are part of the ever-evolving world of cyber information and communications.

Cyberspace - Tactics and Defense

It's been estimated that as many as 80 percent of exploitable vulnerabilities would be mitigated with basic cybersecurity hygiene, such as patching, antivirus updates, password management, and other techniques. These simple tasks do not require huge investments or large information technology staffs, but they do require greater awareness. That is our goal with the summaries included here.

Cyberspace - Legal

This section covers legislation and law enforcement efforts aimed at maximizing the risk experienced by cybercriminals. In addition, the legal consequences of cyber crime are included here.

Cyberspace-Related Conferences

Within this section, we provide a list of events -- with a link to the conference home page – that focus on cybersecurity and provide attendees an opportunity to further increase their awareness and education. Organizations are encouraged to submit events through NSCI (cyberpro@nsci-va.org). There is no cost for listing events in this section.

Cyberspace-Related Training Courses

This section provides information on cyber-related training courses offered by various vendors.

Cyberspace Business Development Opportunities

In this section, we provide information regarding cyber-related business opportunities as published by Federal Business Opportunities (www.fbo.gov).