John Bruce Wallace

Cyberwar the Weak Link in the Infrastructure

September 11, 2001 (9-11) has left an indelible impact upon the security awareness of the United States. In 2003 the Public Broadcasting System (PBS) aired a Frontline program that focused on the issue of Cyberwar, examining through the opinions of several different experts our security and preparedness for attack in the face of constant, unseen threats. The program focused discussion on the subjects of Cyberwar, terrorism, and the issues of security as applied to the various elements that have been considered the essential infrastructure of the United States as a society. Elements of the infrastructure examined included by were not limited to: power grids, municipal water supply systems, financial networks and systems, the Internet, corporate and government networks and systems, transportation systems, energy transport systems, the military and its logistic and command systems, with particular attention on the technological information systems such as Supervisory Control and Data Acquisition (SCADA) digital systems that form the heart of these infrastructure elements. The overriding question that one comes away from the discussion with is: What part of our infrastructure is most vulnerable?

In the immortal words of Walt Kelly's comic character Pogo, "We have met the enemy and he is us" (http://www.igopogo.com/we_have_met.htm). Unfortunately we have not understood Sun Tzu's perception that one must understand one's enemy as one understands one's self. For we have mis-understood the importance of understanding the frailties of mankind and how these faults have come to haunt us. The elements that comprise the infrastructure are but tools that represent *use options* designed to address and meet the needs of humanity. While it is true that the various elements of the infrastructure have their strengths and respective weak points, the creation and sustenance of the infrastructure and its qualities rests squarely on humanities shoulders. Look! what we have made in our image! The most vulnerable part of our infrastructure is not actually part of the infrastructure, but rather is present to and interactive with all aspects of the infrastructure. The weak link is the human element. It pervades all other aspects in a number of ways including but not limited to:

- Humans design and develop the software used throughout the infrastructure
    - Designed and developed the software used in the SCADA system(s)
    - Designed and developed the operating systems, applications, middleware
    - Designed and developed the protocols for network communications
    - Designed and developed the viruses, Trojan horses, and malware that represents the threats to the vulnerabilities of the infrastructure
    - Designed and developed the various administrative tools, such as Ethereal, that both benefit the administration of the infrastructure, and provide opportunity to hack and attack the systems, exploiting vulnerabilities
- Humans conceived, designed, and developed the various elements of the infrastructure
    - The power grids
        - Physical power lines
        - Power plants
        - Above and below ground transmission facilities
    - Pipelines, energy transport systems

    - Transportation systems and facilities
        - Airports
        - Railroad systems
        - Highways
        - Mass transport systems
    - Water supply systems
    - Communications systems
    - Military logistics systems
    - Various Wide, Metro, and Local area networks
    - Various management, supply, inventory, order and shipment, financial, data storage, server, office suites, and routing software programs and applications utilized in the daily administration of the various infrastructure systems including and in addition to SCADA
- Humans designed and developed the hardware that runs the infrastructure
- They manage the physical locations of the various physical element s of the infrastructure
    - manage and maintain power-plants
    - physically build the facilities
    - establish the policies that govern the implementation of the systems
    - determine the acceptable levels of security
        - write security policy
        - evaluate potential threats
        - respond to attacks
        - establish acceptable levels of risk
        - bottom-line the financial parameters
    - influence the cultural mind-set
    - created and maintain the Internet
    - developed and maintain various private, corporate networks
- Humans work at the infrastructure locations
- Humans are the corruptible element
    - They are open to bribe
    - They are amendable to the influence of charismatic leaders
    - They are willing to fight for a perceived worthy cause
    - They are willing to explore off-limited areas for fun or profit

    - They are willing to trade security for profit
    - They are willing to spite their nose to save their face
- Humans are the most unpredictable element
- Humans are the most dangerous element

While the discussions in the Frontline feature revolved around the vulnerabilities associated with the various elements of the infrastructure, the focus always ended with discussion of how humans were acting or could potentially act in the various scenarios that were the subject of debate. For instance, the issue of the vulnerabilities of software and SACADA focused on many human failings including but not limited to:

- Inability to reliably determine the trustworthiness of potential job applicants
- Un-willingness of senior corporate officials to reduce profits in order to increase security
- The limited ability of systems analysts, engineers, and programmers to produce bug free software
- The limited ability of systems analysts, engineers, and programmers to produce network connections for the multiple proprietary systems that have been melded into SCADA
- Inability of or un-willingness of governmental leaders to adequately meet the task of mandating implementation of adequate across the board security
- Historic failure of industry and governmental leaders to perceive the nature and degree of threats and attacks, and their associated risks
- Inability of corporate and governmental leadership to understand and prepare for the potential major threats

While the intense scrutiny focused on the various components of the infrastructure since 9-11, has disclosed untold instances where we are vulnerable, as well as strong indicators that excellent improvement has been made in the implementation of greater security, the focus ultimately comes back to the human element. One focal point that has gained attention since 9-11 is the type of mind-set that lies at the heart of the terrorist beast. As Socrates observes to Crito, "For he who is a corrupter of the laws is more than likely to be a corrupter of the young and foolish portion of mankind" (Plato). A description that accords with Al Qaeda and many other terrorist recruitment tactics. While this certainly provides an insight into one of the human flaws underling our infrastructure vulnerabilities, there are many others that reside right here with our own organizations and culture.

As the numerous interviews and assessments indicate the flaws in software, lax physical security measures around the physical property associated with the various infrastructure components, slow uptake and response to staged and real attacks, failure to recognize potential attack scenarios, inability to see the future with clairvoyance are all human frailties. More specifically, with the current threats from Al Qaeda we are dealing as noted with Plato's un-ethical being as mentioned in the *Crito*. The flaws of mankind underlie the flaws that are now perceived as the infrastructure vulnerabilities that we as a society are fearful will be exploited to our detriment.

As pointed out by numerous interviewees in the Frontline feature, cultural change to emphasize the tremendous importance of security and the practice of secure policy in every aspect of our inter-cultural exchanges has become essential. But this is not the easiest of tasks; in fact it has been our struggle across history. Our ability to stay one-step ahead of ourselves is most taxing. The risk evaluations that are routine now in many of the infrastructure systems still weight the trade offs of profit *vs*. security, with uncertain results. New developments in security present new challenges to those that gain some sense of value from compromising those security features, just because they can: A mind set that is hard to battle, let alone reach some conclusive victory over. As the old adage goes, Locked doors only keep honest people honest; the willful intruder will find a way in. Constant vigilance is mandatory with uncertainty of success a constant concern. Ultimately the security of the infrastructures is only as good as we are on an average day. This is basically how it has been and most likely how it will continue save some great awaking on the part of most of us to the necessity of security that rests in due diligence on the part of each and not on excessive regulation that may stifle innovation and creativity so badly needed to keep one-foot up on the enemy. How to accomplish this is a major problem that education can only partially address. But, here we have fallen into one of the human flaws that underscore the problem in the first place the ability to balance risks and implement socially advantageous policy. Ah, in the words of Nietzsche, Human, all too human.

References:

I Go Pogo (n.d.) Retrieved July 20, 2006, from http://www.igopogo.com/we_have_met.htm

Nietzsche, F. (1996/1986). Human, All Too Human. Cambridge, England: Cambridge University Press

Plato. (1966/1959). Crito, In C. Shrodes & J. Van Gundy (Eds.). B. Jowett (Trans.) Approaches to Prose (pp. 353-365). New York, NY: The Macmillan Company

Public Broadcasting Service (PBS). (2003, April 24). Frontline: Cyberwar. Retrieved June 19, 2006, from http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/

Sun Tzu. (2002).The Art of War. Mineola, NY: Dover Publications