Testimony to
The Subcommittee on Research and Science Education, House Committee on Science and Technology, on the topic of "Cyber Security R&D"

Testimony of Anita D'Amico, Ph.D.

June 10, 2009

Introduction

Thank you Chairman Lipinski, Ranking Member Elhlers, and members of the Subcommittee for the opportunity to testify on this important topic.

I am the Director of the Secure Decisions division of Applied Visions, Inc. I was educated as an experimental psychologist; applied my skills as a human-factors psychologist in maritime ship operations, manned spacecraft and surveillance aircraft; and for more than 15 years have been involved in various aspects of cyber R&D. For the past nine years I have been directing the Secure Decisions division of AVI to enhance the situational awareness of those defending our critical computing infrastructure.

As a small business engaged in custom software development, Applied Visions recognized over a decade ago the frailty of our country's IT infrastructure and the importance to our country of instilling and monitoring good cyber security practices. AVI invested in a new division dedicated to improving the situational awareness of those responsible for defending our critical IT infrastructure. In under ten years the Secure Decisions division has become, even as a small business, a leader in cyber situational awareness R&D.

We perform R&D sponsored by the Department of Defense, the Intelligence Community, and the Department of Homeland Security. And from my perspective one of our most valuable contributions is when we transfer that R&D into usable products for use in both DoD and in industry. We publish research results – those that we are permitted to disseminate – in peer-reviewed journals. We partner with large companies like Raytheon and ITT, universities including Johns Hopkins and George Mason, and other small businesses.

We owe our continued growth in cyber security research in part to the US government's *Small Business Innovation Research* (SBIR) program. Our company is a testimony to the valuable role that SBIRs play in transforming cyber security research into operationally usable software systems and products. Unlike many federally-funded R&D programs that have little accountability for the ultimate operational utility of their research, the SBIR structure holds us accountable for – and rewards – the transition from early stage innovative concepts to

context in which they regulate and prosecute. The law generally has lagged far behind technology; we need technology-savvy courts to keep pace with the changing landscape. Few lawyers are sufficiently schooled in technology and security issues to be able to understand the problem well enough to decide whether or not proposed solutions to the problem are legal – and as a result, the usual answer is "no".

And finally, we must educate the rest of us – the teeming masses who actually *use* the software and cyber infrastructure of the nation – in how to better understand the risks associated with that use, and how to make better decisions.

The cornerstone to this good security decision-making is our understanding of risk. Like most of life, security is about making decisions and choosing between options – making trade-offs between security and convenience, risk and comfort, safety and freedom. Overall, we're not bad at making security trade-offs.[3] The problem we have right now is that our understanding of risk, our basis for making these choices about security, is still based primarily on our physical environment and life as it has been for thousands of years. Our ability to understand, evaluate, and react to risks has not yet acclimated to our *current* environment, meaning the realities of the 21st century and cyberspace. Our *perceived* risk and the *actual* risk do not match, and we often make the wrong decisions as a result.

Therefore, part of raising the awareness of our citizens is to educate them in the actual, rather than the perceived, risks of traveling through cyberspace.

The State of Cyber Education

The current approach to cyber education falls far short of adequately preparing this universe of developers, practitioners, and users for life in the cyber world. Current education is focused on training security practitioners and educating computer scientists, but little is being done for all of the other roles: security practitioner, home user, business owner, software and hardware designer/developer, policy-makers, legal professionals, and even young students using the internet.

Emphasis on Technology and Not People

Information security is often said to be about "people, process, and technology." Technological change can almost be taken for granted, given the natural inclination of engineers and technologists to constantly improve things. Instead, *changing how people think and the process by which we go about doing things should be our primary concern*. We *should* be developing a new breed of multidisciplinary cyber security experts educated in the areas of *people*, such as psychology and organizational behavior, and *processes*, such as management, business process, and the law.

[3] Schneier, Bruce. (2008) *The Psychology of Security*. http://www.schneier.com/essay-155.html, Published Online

Educational Challenges in the Military

The military is also wrestling with this problem, although from a different perspective: they see the need for cross-disciplinary education to incorporate the social sciences into cyber operations in order to better understand the impact of cyber operations on both friend and foe – a form of "battle damage assessment" for cyber warfare. This interdisciplinary approach needs to become the norm rather than the exception: cross-disciplinary education needs to be not only encouraged, but required.

The DoD faces other educational challenges that are somewhat unique to their organizational model. In fact, there are two characteristics of the DoD model that work together to make things quite difficult: incoming technical staff are more often chosen by aptitude than by experience, so that training must start at the most rudimentary level. And, the military tends to rotate people through posts on a regular basis, so that once they achieve some level of competency in cyber security they are likely to be transferred to some other discipline. This is further exacerbated by the fact that technical positions – such as Computer Network Defense – are not known to be a path to advancement (as opposed to traditional combat roles), and hence suffer high turnover.

Conti and Surdu[5] cite these challenges, among others, in their rationale for creating a fourth branch of the service – a peer to Army, Air Force, and Navy – to take on Cyberspace. This has cultural significance. They propose that top-notch cyber talent will clamor to join a service where cyber excellence is viewed as a path to advancement, and where just being a member of that service is a point of pride (as the Marines have achieved with their image as "The Few, The Proud..."). They observe that many young technically-talented individuals make critical decisions in their formative years that influence the direction of their lives. Perhaps the most important decision made by these rising cyber stars is whether or not to engage in illegal activity, like hacking. Creating an elite cyber organization, complete with positive role models, will give these people a chance to make the right choices in their lives.

Educating the Practitioners

Security practitioners have traditionally been *trained* rather than *educated*: the emphasis has been on the practical application of tools and techniques to defend the network, rather than on gaining understanding of the principles and behaviors that inform cyber security. The "old guard" practitioners learned about computer security *after* their formal education was completed, through a form of on-the-job-training as they "wrote the book" on security best practices in the early years. Current practitioners may have had *some* formal education or training, perhaps a degree in computer science or a few courses that led them to obtain some certification, but most of their real learning still happens on-the-job. What neither group realizes is that much of that on-the-job training – which they view as "learning the ropes" with tools and techniques for security – is in fact teaching them about the behavioral and social characteristics

[5] Conti, Lt. Col. Gregory and Surdu, Col. John "Buck". "Army, Navy, Air Force, and Cyber – Is it Time for a Cyberwarfare Branch of the Military?" *IA Newsletter, Vol. 12 No 1*, Spring 2009, http://iac.dtic.mil/iatac.

Systems sometimes fail because the engineers considered a very narrow range of threats; again, the issue is a lack of understanding of the actual risks in the modern world. Information security needs to be an integral part of the core curriculum of computer science for both programmers and engineers. We must teach software developers and systems engineers how to go beyond just functional requirements in the design phase. They need to understand and anticipate all of the ways that experts and non-experts may use their systems. Usability and security testing needs to be performed side-by-side with functional and performance testing during development; students need this as part of their basic education.

Educating the Users

The most difficult audience to get a handle on, but one that desperately needs more education, is "the rest of us" – all of us who use these technologies, who suffer the consequences of failed security, and who all-too-often serve as unwitting accomplices to an attack.

We Need Realistic Test Data

Another challenge relevant to the whole educational and research spectrum is the need for more realistic testing and evaluation of cyber technologies and processes. In most disciplines some form of real-world experimentation eventually becomes practical and necessary; for example, psychologists can evaluate human subjects and compare the results against control groups. In the cyber world this is exceptionally difficult: one cannot perform security experiments on an operational network (let alone on the internet), yet "simulating" such an environment is a huge challenge. Many researchers have built small-scale simulated networks in the lab, but the human element – real people using the network for real tasks – is completely missing and quite difficult to simulate. Realistic training and test data that can scale to the size of large networks is needed to add operational realism to training and research, and to increase the applicability to real world conditions and the potential transfer to implementation. With this sort of realistic simulation and test data we can properly prepare practitioners and developers to operate in the cyber world; without it, they have no other choice but to "learn by doing" in the "real world," with risks and inefficiencies that implies.

The Contribution of Social Sciences to Computer Security

The social and behavioral sciences can play a valuable role in studying and changing the various cultures – software developers, college students, and especially home computer users – so that individuals and societies engage in secure practices almost without ever thinking about them.

We need to understand why our perception of security risk does not match reality. Risk perception is critical to helping us understand how to motivate secure behavior, make better decisions, and create policies that discourage destructive or invasive behavior through real consequences.

We need to apply what we know about cultural influence to creating cultures that are supportive of secure and private computing.

them to their monitors for all to see. There are some encouraging sparks of innovation in this area: for example, graphical passcodes[8] for user authentication. These new types of password, which use pictorial elements, take advantage of people's visual memory recall and are remembered better than meaningless strings of alphanumerics.[9] This sort of forward-thinking research needs to be applied across the entire security problem.

Need for Research on How People Value Information

The crux of information security is securing information that has been designated as valuable. Nevertheless, we have little understanding of what makes information valuable to people. Security practitioners tend to "guard the perimeter," treating everything within the boundaries as if it is of equal value. Yet all information assets behind a firewall are not equal. Some workstations or servers are more valuable than others – perhaps because of the role of its user, the content of its storage device, or the service it provides to the enterprise. People want to protect the most valuable information; yet there are no metrics or even basic insights into how the value of information is determined.[10]

If we knew how to *measure* the value of information, we would be able to apply security measures that follow the high-value information, even as it moves through a network. Just as the President's bodyguards follow him as he moves, so too should security be able to move along with important information. If US network defenders can provide greater protection to the most valued assets, adversaries may be deterred by the extra time and resources required to break into well-protected cyber assets. Of course, this requires the defender to know which information systems contain high-value information – something that is difficult without methods to value information and the means to locate where the high-value information currently resides in a dynamic network configuration.

If we better understood how *people* placed value on information, we would be able to use that valuation to motivate individuals to comply with security practices and change the culture of security. We could also use that understanding of information value to support the calculation of the Return on Investment of security. The ability to recognize and quantify the value of information resident on a network will help security practitioners better secure and protect information and network assets, allow cyber defenders to prioritize their defensive actions by focusing on the most critical network assets, and allow business owners to immediately assess the impact of an attack on those assets.

Understanding the relative value of information underlies all of these decisions. But there is no current methodology used in the DoD for assigning an actual value to information. Current

---

[8] http://www.passfaces.com

[9] Johnson, K. & Werner, S. (2008) . Graphical user authentication: A comparative evaluation of composite scene authentication vs. three competing graphical passcode systems. In *Proceedings of the 52nd annual meeting of the Human Factors and Ergonomics Society*. New York, NY.

[10] Stevens, J. (2005) *Information Asset Profiling*. Pittsburgh, PA, Carnegie Mellon University.

education and research has been on the development of technology within the academic environment of computer science and electrical engineering. This needs to change.

Broaden the Base of Those Receiving Cyber Security Education

The current approach to cyber security education falls far short of adequately preparing the universe of people who every day take actions that make our computing infrastructure more or less secure. We must offer information to – and influence the behavior of – software developers, business owners, soldiers maintaining network-centric systems, policy-makers, lawyers, students, and home-users. The source of this education must go beyond college computer science courses. The education and training of security awareness, good practices, and cyber ethics should start in our elementary schools and extend beyond the academic environment into the training programs offered by professional organizations.

Schools of law and law enforcement must not only teach cyber law and policy, but teach the foundations of the internet and computer usage that underlie the laws and policies.

Social science experts in cultural influence should be consulted on how to raise our national awareness of cyber risks and change the security practices of average Americans.

Experts in learning should advise the retiring old guard security practitioners on how to effectively mentor new security professionals and expedite the transfer of their corporate knowledge.

Computer science curricula must include building security into the entire lifecycle of software development.

We must increase the number of US citizens who master the math and science needed to advance cyber security technologies, and who enroll in advanced degrees in information security.

Use Interdisciplinary Approaches to Make the Cyber Culture More Secure

Changing how people value security and behave with computer systems and networks should be a primary concern of our cyber education and research. It is clear that technological change will happen; it already does. But safe and ethical behavior is not keeping pace with the pervasiveness of computing for work, entertainment, and socializing. Interdisciplinary approaches, which combine computer science with the more people-centric disciplines of psychology, sociology and anthropology, can extend our understanding of how to create a more secure computing culture.

We need research on how people value information. Understanding how people place value on information will help security professionals to motivate compliance with security practices; it will inform the security architects on where to place the greatest defense; and it will form the foundation for security metrics.

Increased the Private Sector's Voice in Cyber Security Education and Research

The private sector, which is a conduit both for attacks on our critical information infrastructure as well as the prevention of those attacks, has no significant influence on the federal R&D agenda in cyber security. Security practitioners in the private sector, where they can influence US workers and businesses, are neither consulted on the national agenda nor given easy access to the results of federally sponsored R&D. This can be addressed in several ways:

- The sponsors of cyber security R&D should conduct outreach activities to professional societies of security practitioners including ISSA, ISACA (*Information Systems Audit and Control Association*), and (ISC)2 (*International Information Systems Security Certification Consortium*).
- Researchers must be encouraged by the sponsors of their research to publish the results of their work in trade magazines and on-line forums where private security professionals communicate.
- The government should incentivize the private sector to bring interns from academia into their IT infrastructure to gain on-the-job experience prior to their graduation.
- ISACs should be used as a medium for connecting private sector needs with federally funded research.

In sum, there are many substantive ways in which the social sciences can assist us in improving cyber security. My thanks to the Committee for allowing me an opportunity to share my viewpoints.

Acknowledgements

I would like to acknowledge the contributions of Laurin Buchanan and Frank Zinghini of AVI, and Geoff Mumford of the American Psychological Association, to the preparation of this testimony.

ANITA D'AMICO, PH.D.
Director
Applied Visions, Inc. – Secure Decisions Division

Dr. D'Amico is the Director of *Secure Decisions*, a division of **Applied Visions, Inc.** She is a human factors psychologist and an information security specialist, with interests in improving situational awareness of information security analysts through visualization and cognitive analysis. Her most recent work has been in the area of combining geographic information with network security and network management information to improve security and preserve continuity of operations.

Dr. D'Amico joined Applied Visions in 2000 to help create and grow the *Secure Decisions* division, building upon information visualization technology developed by Applied Visions under an Air Force research contract. The Secure Decisions division of Applied Visions is now recognized as a leading provider of information visualization research and technology development to the Department of Defense, the Intelligence Community, and the Department of Homeland Security.

Prior to joining Applied Visions, Dr. D'Amico ran the Information Warfare Group for Northrop Grumman, where she was responsible for developing that new business area. In the years before that she had applied her human factors and psychology training to a variety of domains, all centered about the interaction between humans and machines, including such disparate domains as aircraft design and ship handling.

Dr. D'Amico has published widely on the topic of cyber security, particularly from the perspective of human factors and the impact of situational awareness on the effectiveness of cyber security practitioners. She is a frequent keynote speaker on the topic at industry conferences, and she chaired the 2003 Forum on Information Warfare, presented by the Management Information Systems Training Institute, Washington, DC. Recently, she conceived and conducted a joint industry/government workshop on understanding and determining the impact of cyber security breaches on organizational mission.

Dr. D'Amico received a B.A. from the University of Pennsylvania, and an M.S. and Ph.D. in psychology from Adelphi University. She served five years as a member of the board of directors of the New York Metro chapter of the Information Systems Security Association (NYMISSA).