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

prototype development and technology transition planning, all within a typical SBIR lifespan of three years.

The Human Element in Cyber Security

We named our division "Secure Decisions" to recognize the importance of *human decisions* in cyber security. As a psychologist working in a field predominated by computer scientists, I chose a name that reflected our goal to enhance the *situational awareness* and decision-making of cyber security practitioners. Of course, security practitioners are not the only individuals whose decisions make our critical computing infrastructure more or less secure. Many others, including home-users of computers, policy-makers, cyber lawyers, software developers, and educators, make us all more or less secure through their individual actions.

The current emphasis in cyber security R&D has been technological: creating or improving tools to enforce security. While this is indeed necessary, there is a significant *human* element to the problem that cannot be ignored. As researchers and educators, we must address all the many different roles that we humans play in cyber security, beyond just the security practitioner who administers firewalls, tunes intrusion detection systems, and monitors networks. We must also educate the software developer, lawyer, policy-maker, and all of us users who are unwitting accomplices of the attacker. The recommendations in the Cyberspace Policy Review just issued by the White House[1] recognize this.

Let's look at the software developer as one example of the need for enhanced security education. From the very start of the software life-cycle – creating the software itself – software developers are inadequately schooled in how to program securely; security is often added on afterwards. Rewards are given for speed to market, not for creating secure software. For example, just *two* programming errors resulted in more than 1.5 million web site security breaches during 2008.[2] And all too often, the developer's initial response to the discovery of a vulnerability is something akin to "gee, we never thought a user would do *that* with it." We must change the way that programmers go about understanding the needs and behaviors of us as users, and in creating the software that we use.

Technical solutions must be easily deployable and usable. Gaining a deeper understanding of how people use technology by bringing together computer science and the behavioral sciences can make our technological breakthroughs actually useful and relevant to society.

We then must educate the cyber policy-makers and legal professionals in the fundamentals of confidentiality, integrity, and availability of information systems so that they understand the

---

[1]Cyberspace Policy Review (2009)
http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
[2] SANS Security Leadership Essentials for Managers: Experts Announce Agreement on the 25 Most Dangerous Programming Errors - And How to Fix Them, January 12, 2009
http://www.sans.org/top25errors/?utm_source=web&utm_medium=text-ad&utm_content=Announcement_Bar_20090111&utm_campaign=Top25&ref=37029

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

There has indeed been an increase in the number of academic institutions offering undergraduate and graduate degrees related to cyber and information security, but the majority of these programs are still technology-focused: computer science, computer engineering, electrical engineering, and so forth. *This is not enough*. Technology can shore up our defenses, but an emphasis on the *social* sciences can change the way we look at things: how we as a society view the risks and trade-offs in the digital world, and how we make those day-to-day decisions that have such a significant impact on the safety of our travels in cyberspace.

Unfortunately, there are not many examples of the collaboration between the social sciences and the computer sciences required to achieve this shift in education. Conferences like the *Workshop on the Economics of Information Security* and the *2008 Workshop on Security and Human Behaviour* are initiating a dialogue between technologists and social scientists, and we are beginning to see encouraging signs of this collaboration at the educational level. In addition, a workshop next month at the National Academy of Sciences, *Usability, Security, and Privacy of Information Systems*, is focused on identifying new research areas in "usable security" and will influence the research agendas of both NSF and NIST, which are sponsoring the workshop.

Visionary leadership is needed to achieve these changes in educational philosophy. As long as technology is viewed as the end-all of cyber security research and education, the focus will remain on problems in that area. And even if technology development remains the focus of our cyber security research and education, we have several major hurdles to overcome. One hurdle is the shortage of US citizens who are acquiring the requisite math and science skills needed to teach and conduct hard research in cyber security.[4] This leaves many of the hard technology questions unanswered by our own citizens. Another hurdle – and this one I feel very strongly about – is the limited transfer of research findings into real-world use. Advanced education programs (such as for a Ph.D. in Computer Science or Information Systems) emphasize *publication* rather than transfer of findings into real practice. The system of grants that fund the work of students and their professors places more value on prior publications than practical results. We need to transition the research into the everyday world of Information Technology.

There are encouraging examples of such visionary leadership in interdisciplinary security. New York University, for example, recently merged with Brooklyn Polytechnic University, and quickly set out to build bridges between their engineering and social science communities. They now have a program combining Economics with Computer Science. Georgia Tech Information Security Center (GTISC) also recognizes the importance of interdisciplinary studies, and has launched a cooperative effort between their College of Computing and the Sam Nunn School of International Affairs. Despite these forward-thinking programs, there are few if any educational opportunities in cyber security that combine psychology, anthropology, or sociology with computer science.

[4] Zweben, Stuart. Computing Degree and Enrollment Trends, from the 2007-2008 CRA Taulbee Survey, 2008, at 4, www.cra.org/taulbee/ CRATaulbeeReport-StudentEnrollment-07-08.pdf

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.

of their adversaries. The newest, upcoming generation is indeed getting more-formalized education – for example, an MS in Information Security is now an option at many universities – but they lack the *context* for that education. Without real-world experience, and without including behavioral and social sciences in their education, they too will not gain a real understanding of the problems or of their adversaries until they have been on the job for a while.

A few years ago we had an opportunity to conduct a formal Cognitive Task Analysis of nearly eighty information assurance analysts in the DoD and the Intelligence Community.[6,7] We learned from that analysis that *mentorship* of network defenders is very important. Rapidly transferring corporate knowledge typically acquired through years of experience from old guard to new guard will be particularly important in the coming years as the first generation of network defenders retires. One area ripe for research is how to improve this mentorship to maximize the value of learning from the more-experienced to the less-experienced practitioner. Social science work on learning, mentorship, and collaboration can serve this need.

We also learned that the *personality characteristics* of entry-level network defenders are perceived by experts as equally or more important than their technical education. Such characteristics as curiosity, perseverance, assertive questioning, and good communication skills were considered strong markers of future success of an entry level defender. How do we select for and train these characteristics in our future cyber workforce to ensure that our defenses are as strong as possible? This is answered by the social sciences as much as by the technical disciplines.

Educating the Developers

The emphasis on "securing the perimeter" of networks is a side-effect of a more fundamental issue: security is all too often an afterthought. We build flawed software and then expend countless resources trying to patch the cracks and shore up the defenses. And when we do build flawed software products, the pressure to bring these products to market causes many to be released before adequate security testing has taken place. All of this raises questions about current software engineering pedagogy.

We need to teach secure coding practices – and, more importantly, we need to convey a fundamental understanding of the importance of security – from the very start, in high school computer science classes. Most of our computer science programs in higher education teach students the fundamentals of developing software and systems, and culminate with students building some hardware or software object, but little attention is generally given to the design and implementation of security within these objects.

---

[6] D'Amico, A. & Whitley, K. (2005). Achieving cyber situational awareness: A cognitive task analysis of information assurance analysts. In *Proceedings of the Human Factors and Ergonomics Society 49th Annual Meeting*, Orlando, FL, pp. 229-233.

[7] D'Amico, A. & Whitley, K. (2007). The real work of computer network defense analysts: The analysis roles and processes that transform network data into situation awareness. In *Proceedings of the Workshop on Visualization for Computer Security*, Springer-Verlag Berlin Heidelberg, pp. 19-37.

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.

Collaborative Techniques

Human collaboration is an important means for analyzing information about potential attacks. There are numerous instances where one government agency or commercial organization was aware of a serious attack but did not have the authority, means or motivation to share that information.

One group working to bridge this gap at the *organizational* level is the *Information Sharing and Analysis Centers* (ISAC) Council. There are several individual member councils that focus on various areas of critical infrastructures, such as Communications and Information Technology, but this group and its members represent the exception, not the norm, and information-sharing is particularly problematic within the government.

But we also must foster collaboration at the *individual* level, and this is where the social sciences can help bring about positive change. Individual network defenders and law-enforcement agents struggle every day to find attackers. Often, several individuals are working at the same time in pursuit of the same perpetrator, but they have no idea of each other's existence or of their common goal. And worst of all, they don't know that each of them holds a different piece of the puzzle that carries the answer. If they had an effective means of communication, whether through online collaboration or shared visualizations, and if they have the understanding that they do not have to – and should not – solve this problem alone, they would be able to work together more effectively. It is at that individual collaboration level that psychology and sociology can play a significant role.

So in addition to all of the effort that is currently being applied to getting *organizations* to collaborate more effectivey (as described in the President's Cyberspace Policy Review), we must also work just as hard to improve the ability of *individuals* to collaborate effectively within and across organizational boundaries. Assuming that policies allow for information sharing, we need to have media in place for collaboration and shared situational awareness.

Usability to Enhance Security

There is a never-ending tug-of-war between security and usability. The more protections that are built into our systems, the harder they are to use. Apple famously lampooned Microsoft's attempts at improving the security of Windows Vista by asking users to "cancel or allow" a wide range of what users perceive as "normal" activities. And human nature being what it is, users do their utmost to find ways of circumventing these controls so they can get on with their work, including developing a knee-jerk response to "allow" everything that comes along.

A lot of attention is being paid to usability of computing systems in general – making applications or web sites more "user friendly", for example – yet the concept is often ignored when security controls are designed in. Think of the most basic problem of remembering passwords. More stringent passwords, requiring nonsensical strings of numbers, letters and special characters, are at odds with people's innate ability to remember short, meaningful sequences of information. As a result, people simply write them down on post-it notes and stick

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.

work[11,12] on cyber information valuation within DoD has advanced the theoretical discussion but remains only conceptual. Metrics are not *usable* unless they have been validated against real-world observations.

Research is needed to better understand how people place value on information, to identify the most promising metrics for valuing information, to apply those metrics to information observed in a real-world environment, and to determine whether or not the conceptual metrics are verifiable in real data.

The Private Sector's Role in the Cyber Security Research Agenda

Security practitioners in the private sector are on the front line of cyber defense. These individuals write the security policies, deploy the technologies, and attempt to compute ROI for security expenditures. They have direct influence on the security practicies of individual US workers and business owners whose inattention to security could have cascading effects on our country's computing infrastructure. Security practitioners deal with the *people* side of security, far more than any of today's educators or researchers. Yet the security practitioners have virtually no influence on the cyber security research agenda and only indirect influence on the curriculum of computer science programs.

The government does not actively solicit input from the private sector in crafting its R&D or education agenda, nor does the government actively promote dissemination of the research results to media and forums usually consulted by private security practitioners. As a member, Board Director, and Advisor of the New York Metropolitan Chapter of the Information Systems Security Association (ISSA) I regularly meet with hundreds of chapter members who are security professionals in New York-based businesses. We have never been asked for input into a national research agenda. Our membership has been genuinely surprised when they've heard about the results of my own work sponsored by DHS, IARPA, the Air Force, and DARPA. Furthermore, these members of the private sector are *willing to participate in the technical transition of the R&D* – but they are rarely asked to do so.

Additionally, the ISACs and other organizations, such as the National Academy of Sciences, could be tapped as conduits for collaboration between the private sector and government in developing the cyber security research agenda.

Conclusion

Effective cyber security is often said to be about "people, process, and technology." Although "people" come first in this description, the emphasis in federally funded cyber security

[11] Grimaila, M.R. and L.W. Fortson. (2007) *Towards an Information Asset-Based Defensive Cyber Damage Assessment Process*, Computational Intelligence in Security and Defense Applications.
[12] Hellesen, D. (2008) *An Analysis of Information Asset Valuation (IAV) Quantification Methodology for Application with Cyber Information Mission Impact Assessment (CIMIA)*, Master's thesis, AFIT

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.

Security must be more usable. Interdisciplinary approaches to usability can make it easier for practitioners to install and tune security technology, and for users to comply with security policies and practices.

Human factors psychologists with expertise in collaborative media should work with computer network defenders to develop effective means for timely information sharing needed to rapidly detect cyber attacks within and across organizations.

The disciplines of economics, business administration, and information systems must study the interdependencies of computing assets and business processes so that accurate ROI for security investment can be computed, and data-driven plans for continuity of operations can be developed.

Foster Technology Transition of Cyber Security Research

The existing research agenda, framed by and for computer scientists, emphasizes publication of research results above technology transition. Little current research and education funding is directed to the operational implementation of the advanced technologies. The problems encountered in getting a technology to work in the real world – accreditation, affordability, usability – are not deemed worthy of peer-reviewed publications and are therefore dismissed by many professors, students, and funding agencies who measure their achievements through publication history.

There is a short supply of US citizens with security-related advanced degrees who can transition technology into the DoD where security clearances are required. Non-academic research institutions who have US citizens to transition technology, such as research contractors or government laboratories, do not have the streamlined Institutional Review Board processes required for technology evaluation studies involving people; hence the human element is all too often left out of the research.

To increase the likelihood of technology transition we must take several steps:

- Realistic, scalable test data must be provided to the researchers by the funding agencies.
- Funding agencies should include measures of technology transition in their evaluation of grants and research contracts.
- Funds should be available for crossing the chasm from prototype to operational deployment. This includes funding for accreditation and usability evaluations.
- The government should foster collaboration between university researchers and non-academic research organizations. The universities can use their Institutional Review Boards to guide corporations and government laboratories in testing new technologies with human subjects. Research companies with personnel who have security clearances can assist universities with technology transition into DoD sites that are not ordinarily accessible to university students and professors.

Increase 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.