

Workshop Summary

Rethinking Cybersecurity: A Systems-Based Approach

**A workshop sponsored by
The Center for Risk Management of Engineering Systems and the
Institute for Information Infrastructure Protection (I3P)**

**Co-chaired by George Foresman, Yacov Y. Haimes, Barry M. Horowitz
and Charles Palmer**

**Darden School of Business – University of Virginia
November 16-17, 2010**

Table of Contents

Executive Summary	1
Background and Rationale	2
Summary of the Workshop Process	3
Session Summaries	
Application-Based Security	4
Opportunities and Risk Posed by Cloud Computing	6
Moving Collaboratively Forward	9
Summary Discussion: The Way Ahead.....	11
Keynotes	
Robert Carey: Cybersecurity and the U.S. Department of Defense	13
Richard Pethia: 20+ Years of Cyber (in)Security.....	14
Mark D. Rasch: Legal and Security Issues in Cloud Computing	15
Marcus Sachs: The 2010 Verizon Data Breach Report.....	17

Acknowledgements

The Center for Risk Management of Engineering Systems and the Institute for Information Infrastructure Protection (I3P) thank the workshop presenters and participants for their expert advice, their openness, and their leadership in the field of cybersecurity. Many thanks also to the University of Virginia Darden School of Business for its hospitality and organizational support.

This material is based in part upon work supported by the U.S. Department of Homeland Security under Grant Award Number 2006-CS-001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P). The I3P is managed by Dartmouth College. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College.

Executive Summary

“Rethinking Cybersecurity: A Systems-Based Approach” took place November 16 and 17, 2010, at the Darden School of Business. Sixty-three people attended the workshop, including representatives from government, industry and academia with experience in critical infrastructure protection, security strategies and business resilience. The event was a joint presentation of the University of Virginia’s Center for Risk Management of Engineering Systems and the Institute for Information Infrastructure Protection (I3P), a research consortium managed by Dartmouth College. Present were representatives from a broad spectrum of organizations, including The U.S. Department of Defense (DOD), the National Aeronautics and Space Administration (NASA), the CERT Program at Carnegie Mellon University, the Johns Hopkins Applied Physics Laboratory, the Stevens Institute of Technology, International Business Machines (IBM), Verizon, Bank of America, and The International Council on Systems Engineering (INCOSE).

The purpose of the workshop was to develop a deeper understanding of cybersecurity in the systems context, and to foster relationships across government, industry and academia that will bring that goal closer to reality. Addressing the problem from a number of different angles over the course of two days, participants probed a fundamental question vexing security engineers: How to make cybersecurity a core function on the system level?

A panel discussion on application-based defenses described an asymmetrical fight pitting the security community’s reactive approach to cybersecurity against global adversaries who are innovative, collaborative and—in some cases—well funded. Large institutions naturally require trusted systems; the challenge is to build systems that are both trusted and agile. Creating systemic defenses requires the cooperation of decision-makers, systems engineers and security engineers. There is a need for better security measurement tools, and security should be treated as a core function.

A panel discussed the considerable security challenges and opportunities posed by cloud computing. Market forces are driving a headlong move toward distributed computing, with little regard for the security consequences. A need exists to define cloud security standards and architecture based on what will benefit the broader community, rather than the expectations of discrete clients. It remains unclear whether government or industry will lead this effort.

A discussion on coordinating the efforts of government, business and academia identified trust as a key component in cooperative action. The panel discussed ways to forge that trust from the perspective of regulators, government and industry. The security community must make a strong business case to garner industry support, and articulate an open public research agenda in order to focus the resources of academia.

Among the primary themes workshop participants identified for moving toward systems-based security were the need for better measurement tools, standards, and the inclusion of security as a core element of business operations. One challenge is to apply order to a cyber infrastructure that evolved rapidly and organically. To that end, some participants advocated a quality-assurance “building code” for cyber. The workshop discussion was a necessary first step that should be followed by discussion with other communities about how to build more secure systems. The key is to find the leverage points to bring about needed change. A first step should be to bring together systems engineers, security experts, business leaders and major customers such as DOD, to begin shaping standards.

Background and Rationale

Current approaches to cybersecurity focus mostly on strategies that address specific vulnerabilities. The purpose of this workshop was to discuss steps that could be taken to develop a more systemic approach that considers all facets of security. Overall, the goal was to foster frank discussion and idea-sharing about systems-based cybersecurity, to identify emerging trends, and map a way toward a more systemic approach. The workshop's 63 participants were drawn from leaders in government, industry and academia with interests in the fields of critical infrastructure protection, cybersecurity and business resilience.

Currently, most cybersecurity technologies rely on perimeter defenses such as passwords, network firewalls and virus protection software. Workshop participants examined security in a more holistic context, incorporating such varied components as domain applications, organizational risks, policy and procedural solutions, and cultural and human factors. The discussions covered such topics as resilience, data integrity, system operator tools and real-time oversight. Participants discussed the unique range of security vulnerabilities and opportunities posed by the advent of cloud computing, as well as legal issues pertaining to the cloud. They discussed ways to foster better collaboration among government, industry and academia in the shared quest for systemic security.

Among the workshop's goals were to:

- Examine how critical system functions fit into a comprehensive security strategy;
- Examine the unique opportunities and security risks posed by the widespread adaptation of cloud computing;
- Facilitate communication and cooperation among cybersecurity professionals and thought-leaders in government, industry and academia who are interested in critical infrastructure protection, security strategies and business resilience;
- Provide a framework for needed research and action going forward.

To that end, the workshop featured keynotes as well as expert panels on current and evolving security applications; the opportunities and risks posed by cloud computing; and formulating a collaborative response to evolving challenges. Robert Carey, Deputy CIO at the U.S. Department of Defense, gave a keynote on the unique cybersecurity challenges confronting the Pentagon. Rich Pethia, director of the CERT Program at Carnegie Mellon University's Software Engineering Institute, presented a keynote on the history of cybersecurity and what it tells us about future challenges. Technology attorney Mark Rasch gave a luncheon address on legal and security challenges in cloud technologies, and Marcus Sachs gave a dinner presentation on the *2010 Verizon Breach Report*.

Summary of the Workshop Process

The workshop took place November 16 and 17, 2010, at the Darden School of Business at the University of Virginia in Charlottesville. The program consisted of three panel sessions, two keynotes, and two summary discussions facilitated by former Department of Homeland Security Under-Secretary George Foresman. In addition, speakers at lunch and dinner Nov. 16 gave provocative presentations on cloud computing and a forensic analysis of cybersecurity breaches, respectively.

Each panel session included presentations by four diverse experts in the subject at hand, followed by a discussion period among all workshop participants. The keynote addresses likewise were followed by discussion periods.

Each day concluded with a wide-ranging summary discussion that included all of the day's topics, and, on the second day, coalesced elements of the entire workshop. Under Foresman's inclusive and probing direction, each of the participants contributed in a substantive way.

The presentations, in chronological order, were:

Day One Keynote: Robert Carey, Deputy Chief Information Officer, U.S. Dept. of Defense

First Panel: Application-Based Security

Lunch speaker: Mark Rasch, Legal and Security Issues in Cloud Computing

Second Panel: Opportunities and Risk Posed by Cloud Computing

Day One Summary Discussion: Facilitated by George Foresman

Dinner speaker: Marcus Sachs, The 2010 Verizon Breach Report

Day Two Keynote: Richard Pethia, 20+ Years of Cyber (in)Security

Session Three: Moving Collaboratively Forward

Workshop Summary Discussion: Facilitated by George Foresman

Session One: Application-Based Security

Moderator: Barry M. Horowitz, Department of Systems and Information Engineering, University of Virginia

Kristen Baldwin, Principal Deputy Director, Systems Engineering, Office Director, Defense Research and Engineering

Jennifer Bayuk, Program Director of the Systems Security Engineering program, and Industry Professor at the School of Systems and Enterprises, Stevens Institute of Technology

Rick Dove, Chairman, Paradigm Shift International

Robert A. Martin, Principal Engineer, the MITRE Corporation

Background:

The panel examined critical system functions and how they affect a comprehensive approach to security. The panelists described an asymmetrical fight, in which the security community builds static artifacts and the adversary community embraces innovation and collaboration. Moderator Barry Horowitz opened the discussion with an anecdote illustrating the cultural difficulty in building systemic security. He had co-authored a paper with panelist Jennifer Bayuk on systemic security, and submitted it to a prestigious systems engineering journal. In the peer-review process, two of the six reviewers asked why a systems engineering journal was even considering a paper about security. The paper is slated for publication in 2011, but the reviewers' response is a blunt reminder of the status quo: Security remains an afterthought to most systems engineers. Decision-makers, systems engineers, security engineers, and academicians all have important roles to play in a cultural shift toward systemic, trusted and agile security systems.

Key Findings:

The Contest is Asymmetrical: A large number of adversaries with little at stake are arrayed against relatively few institutions with a great deal to lose. Those with much to lose—government agencies, banks, industrial facilities—take an insular approach to security. They build walls and act autonomously. Attackers, on the other hand, share freely and embrace innovation. Moreover, they are self-organizing: they exchange information at tremendous rates across domains, they adapt ideas from diverse sources, and they apply them immediately. The security community must become more agile to counter this asymmetric threat.

A Need for Trusted and Agile Systems: Large institutions are not structured for adaptability. Government agencies, and to a lesser extent large business enterprises, place a premium on trusted, purpose-built systems. This careful approach can become a liability in the face of rapidly evolving threats. Institutions also typically design against fixed threats, and their defenses are consequently static and slow to change. Corporations

and other large institutions must pay more attention to the development of systems that are both trusted and adaptable.

A Cultural Shift: Systems engineering has traditionally focused on functionality, and approached security as a standards-based check list. In order to build effective systemic defenses, systems engineers and decision-makers must treat security as a core function, and security engineers must learn to think systemically.

Learn to Anticipate: The security community does a good job of closing vulnerabilities after they have been exploited. It does not do a very good job of anticipating those vulnerabilities and addressing them before they can be exploited. Would better recognition capability confer an advantage in systems security? Are there logical patterns that we can apply in that direction?

Information-Sharing is Critical: Building systemic security is a cultural challenge as well as an engineering one. Developing systemic defenses requires the full cooperation of three distinct communities: decision-makers, security engineers, and systems engineers. These communities have little in common. Decision-makers play a critical role, because the engineers can't build systemic defenses without the resources they control. And the security engineers can't win without the full support of the systems engineering community. Finding a way to build trust and share information among these communities is an important step forward.

Reality Check: Though perimeter defenses have historically been the focus of the security community's efforts, building a completely airtight defensive perimeter is not realistic. Engineers and decision-makers must acknowledge that they can't protect everything. The solution is to develop defense-in-depth strategies that preserve core data and functions even when the perimeter is compromised. Users need to decide—in the context of their overall mission--what they most want to protect, and at what cost.

Measurement Tools are Lacking: The study of systems security engineering is in its infancy. Few scientifically validated tools exist to measure the threat or to evaluate how well defenses are working. Academia has a role to play in developing metrics that help define the scope of the problem and measure the efficacy of solutions.

Need for Systems-Based Training: Because security is absent from system requirements, systems engineers must be trained to recognize threats that must be defended on a systems level. Just as systems engineers and security engineers are divided into separate silos, so is the educational infrastructure.

Tapestry of Tapestries: As defenders identify threats over time, they build or purchase defenses for that specific threat. When new threats emerge, they add new defenses or modify existing ones. As a result, each institution develops its own tapestry of solutions. Historically, when other industries have reached that point, they have applied systems engineering to the complete set of problems. Cybersecurity has now reached that juncture.

Natural Models: In many ways a cybersecurity strategy is akin to an organism's immune system. Cybersecurity systems based on the immune model have existed for some time, but have been unsuccessful because they required too many computational resources to be effective. Now the technology exists to support very robust pattern-recognition capability that mimics natural defenses.

Session Two: Opportunities and Risk Posed by Cloud Computing

Moderator: Yacov Y. Haimes, Director, Center for Risk Management of Engineering Systems at the University of Virginia

Clyde Chittister, Chief Operating Officer, Carnegie Mellon Software Engineering Institute

Tom Longstaff, Senior Advisor, Information Warfare Systems, Johns Hopkins Applied Physics Laboratory

Charles Palmer, Director of IBM's Institute for Advanced Security, CTO for Security and Privacy for IBM Research, and Senior Technical Advisor to the I3P

Greg Shannon, Chief Scientist, CERT Program at Carnegie Mellon University's Software Engineering Institute

Background:

Market forces are driving a rapid move to cloud computing. The cloud provides a pool of configurable computing resources that can be rapidly accessed and managed with minimal effort. The development represents a significant technological advance in cyberspace. Yet the same cloud that has vastly increased the functionality and efficiency of computing has also created multidimensional security concerns. The four-person panel discussed both the security challenges and the security opportunities the cloud poses. Moderator Yacov Haimes posited that the cloud is a pseudo-federation of systems of systems. That sounds complex because it is: The cloud encompasses so many different views, services, and components that we don't fully understand how it operates. Cloud technology also brings to the fore legal, privacy and insider risks. Despite these complications, organizations are moving rapidly to the cloud because of the cost savings it promises. The challenge, then, is to consider these factors in a contextual way that allows engineers and users to make good decisions today.

Key Findings:

The Answer is Not Binary. Security and reliability in the cloud is not an absolute; it falls somewhere on a range from zero to one. Risk is also relative: If a Fortune 500 company's principal rivals assume a risk, it becomes easier for that company to take on the same risk. But if the risk is too great, no one will accept it. We therefore are likely to see a market-driven evolution of cloud reliability and security. Users must decide what

level of risk they're willing to accept in exchange for the access and cost savings the cloud provides.

Get Onboard or Get Out of the Way: The transition to the cloud is driven by market forces, and it is inexorable. Companies that compete with rivals who have embraced the cloud must also embrace it or find themselves at an economic disadvantage. If the cloud contributes to bottom-line profit, the choice not to use it carries certain consequence (a competitive business disadvantage), while security represents a potential consequence. Once companies move to the cloud and let their professional IT staff go, it becomes very difficult to move back. They can recover the data, but not the people.

You Can't Say No, so Make it Work: Security audits will not stop the market-driven movement to the cloud, so cloud security must be treated as a systems engineering question. Security people should not approach security as a compliance mechanism; they should treat it as a design constraint. The few early adapting companies who have used that approach have been extremely successful in working with cloud providers to get the information and controls they need.

Greater Security, at a Cost: The cloud enables new approaches to security. For example, engineers could dynamically switch where data is stored and information is processed, thereby increasing the confidence that an insider would not be able to compromise data or services. Homomorphic encryption also holds promise, though it doesn't yet scale. Such solutions may not be cost-effective, but they could be very secure. Engineers need to make decision-makers aware that these possibilities exist. Organizations will need to determine what cost they are willing to accept for enhanced security in the cloud. If moving to the cloud creates a sufficient cost-savings margin, organizations may be able to spend more on this type of security.

Choice of Cloud Solutions: We speak of 'the cloud' as a single entity, but cloud computing is a broad descriptor for distributed data storage and processing. Users can choose to use public clouds, private clouds, or a mix of the two.

Who Should Lead: Much of the discussion centered on who is leading, and who should lead, the movement to cloud computing. The U.S. Department of Defense, for example, has concerns about protecting sensitive DOD data stored on private industry networks, even if DOD knows where the data is. That issue becomes even more difficult in the cloud environment. The military and three-letter agencies are already building proprietary clouds, but the question remains whether those clouds should be built by private industry for the government, or exclusively by the government.

Virtualization is a Real Security Challenge: Engineers must develop strategies to combat virtualized threats. Hypervisors, the meta operating systems that manage and distribute cloud resources to multiple clients, expand the adversary's attack surface. Researchers at the SANS (SysAdmin, Audit, Network, Security) Institute have shown that it is possible to transverse hypervisors and move from one environment to the other. The security community must move to close that vulnerability and other weaknesses

posed by virtualization. For example, how can a security professional be certain that when a machine goes dormant, an adversary has not put a worm or a time-bomb into it?

Balancing Security with Innovation. Part of the challenge will be to improve security in the cloud without dampening innovation, agility and resiliency. Innovation has been a strategic advantage for the United States, in terms of both security and economic development. The Internet is a clear example: Though many are uncomfortable with the lack of control the U.S. government exerts over the Internet, the policy fosters a free flow of information that cultivates one of America's strategic advantages—innovation in the technology fields.

Design for All Users: A need exists to define cloud security standards and architecture based on what will benefit the broader community, rather than competing to meet the specific expectations of discrete clients. Going forward, the security community should develop a consensus on what those standards should be. Cloud operators should describe what they need in order to build security into their systems. Users should have an understanding of the risks, so they can make informed decisions about the degree of risk they are willing to accept.

The Cloud is a Critical Infrastructure. In 1960, John McCarthy said that computation may some day be organized as a utility. The cloud has brought that vision closer to reality. The cloud may soon be designated a national critical infrastructure, on a par with the electric grid and the interstate highway system. Some workshop participants believe it already is a critical infrastructure, even if not yet formally declared as such. In the long term, discrete clouds could merge into a single backbone of collective computing. In that environment, users would have to make a conscious decision whether to keep information out of the cloud, a choice analogous to generating one's own electricity to avoid the risk of blackout.

Ready or Not, It's Here: Decision-makers are driving the move to the cloud for economic reasons, whether or not the security infrastructure is ready. Over the last 18 months, Vericode studied software applications to determine whether they were cloud-ready, and 60 percent of them were not. Vericode did not report how many of those applications were deployed anyway.

Session Three: Moving Collaboratively Forward

Moderator: George Foresman, President, Highland Risk and Crisis Solutions

Lynn McNulty, CISSP, McNulty and Associates

Gregory Garcia, Senior Vice President of Cybersecurity and Identity Management, The Bank of America Corporation, and former Assistant Secretary for Cyber Security and Communications for the U.S. Department of Homeland Security

Rob Pate, Chair of Coordination Awareness, Training and Education (CATE) Committee, Chief Security Officer at Renesys; and formerly with the Department of Homeland Security.

Background:

In opening the workshop's final panel discussion, moderator George Foresman noted that participants had identified a host of systemic security needs, and challenged participants to suggest actionable solutions to those vulnerabilities. Much of the discussion keyed on coordinating the efforts of government, business and academia. Trust was identified as a key component in facilitating cooperative responses. The panel discussed ways to forge that trust from the perspective of regulators, government and industry. Are there effective ways, for example, to create new organizational structures and support tools that enhance resilience and therefore deter prospective attackers? Topics included the sharing and understanding of alternative organizational models, the implementation of system management strategies and opportunities to enhance resilience through research and development.

Key Findings:

Make the Business Case: When decision-makers in business and government evaluate their enterprises, cybersecurity is only one variable among many. Challenges to business-to-business and business-to-government collaboration include black holes, classification issues, and need to maintain competitive advantage in other areas. For example, how can industry share information with the government in a non-regulatory way that enhances collective awareness and response to vulnerabilities? Security professionals need to make the business case for better security practices. That includes the internal business case (greater efficiency; reduced risk) and the external case (because customers and government regulations demand it).

People, Process, Technology: An effective, systemic security strategy must include three core elements: people, process, and technology. A system that lacks any of those core pieces cannot manage the complexity of the cybersecurity challenge. The personnel piece includes academic and professional training, trust relationships, and management. People must know what they're responsible for, and why. Process defines the rules of engagement. For example, which applications can be used in a given environment, and which cannot? Technology is both the tool and the target. In other words, the tool we're using to protect ourselves is the same tool that's being used to exploit us.

Trust is Built on Relationships: Effective collaboration is facilitated by removing barriers and building trust relationships. As Assistant Secretary for Cyber Security and Communications for the U.S. Department of Homeland Security, Garcia worked to establish the National Cybersecurity Communications Integration Center (NCCIC), a 24-hour watch-and-warning facility where senior representatives of major government agencies and critical infrastructure industries sit side-by-side. Organizations with a seat in the room include the National Security Agency (NSA), the U.S. Secret Service, the

Federal Bureau of Investigation (FBI), the Defense Cyber Crimes Institute (CCCI), the Department of Homeland Security (DHS) and various Information Sharing and Analysis Centers (ISACs). The NCCIC is based on the premise that people who work closely together will develop a high degree of trust and collaboration, and share information that that they would not share over email or over the phone.

Role for Educators: The academic community has a big role to play, both in technology and engineering and in the development of training, standards and measurement. In order to focus academic resources, an open public research agenda needs to be articulated. Such an agenda would encourage solutions from the bottom up (ideas generated by operators and security people) and from the top down (vision and architecture). As Foresman noted, university researchers have a plethora of potential solutions waiting for the venture capital required to bring them to market. Educators and industry groups such as the International Council on Systems Engineering (INCOSE) can help set the field for systems security training. Why, for example, are security standards not included in the handbook of processes for systems engineering?

Budding Infrastructure for Cooperation: The industry has made some progress in building forums to monitor and protect against collective vulnerabilities. Examples include Information Sharing and Analysis Centers (ISACs) in industries such as financial services, health, communications and the defense industrial base. With organizations such as the National Organization of ISACs and the Partnership for Critical Infrastructure Security (PCIS), this sharing takes place on the sector-to-sector level, rather than company-to-company. We should encourage these efforts to evolve and strengthen.

Summary Discussion

Facilitator: George Foresman, President, Highland Risk and Crisis Solutions

During the workshop's final session, Foresman asked each participant to summarize key themes from the workshop, provoking nearly two hours of spirited and probing discussion. Among the primary themes were the need for better measurement tools; universal standards, and the inclusion of security as a key element of systems engineering. Several participants emphasized that change is market-driven. A number of participants observed that the discussion was less about systems-based solutions than they had anticipated—a fact that underlined the need to foster a more systematic approach.

Key Findings:

Defining the Threat: Asked to name the greatest cybersecurity threat, most workshop participants looked inward. Among the answers: complacency (for example, some people think that because their systems are not connected to the Internet they are not vulnerable); uncertainty (lacking the flexibility to defend a threat that is impossible to anticipate); and cyber-physical vulnerability, as in process-control systems that can be hacked.

Chaos is Not a Theory: The cyber infrastructure has evolved rapidly and haphazardly, resulting in a widespread and disorganized entity that defies organization. As one participant observed, we should have built a systemic defense from the ground up, but we didn't. Because we didn't understand the technology or apply systems organization (in part because we couldn't measure it), security has evolved in the cheapest, fastest, most unorganized way possible. Fortunately, we now have a better (though still incomplete) understanding of the space and can begin applying engineering standards to cyber infrastructure. A useful analogy can be found in civil engineering codes, which draw on a large body of experiential knowledge. Cyber needs to develop its own set of quality assurance "building codes."

Find the Leverage Points: Secure systems won't be built by security engineers alone; discussions must take place with other communities about what is needed to build such a system of systems. The challenge then is to find the leverage points, which--in this context--are systems engineers and the marketplace. The next generation of security won't come about until systems engineers buy in, because they have to enable the architecture, define the concepts of operations, and accept the tradeoffs. Customers are another leverage point. For example DOD can set the standard for security because it is a large customer, and developers have to accept the standards it sets in order to win contracts.

It's About People: The importance of human factors was a recurring theme throughout the workshop, and several participants reiterated that point in the summary session. How, for example, can we engage a broad user constituency in cybersecure practices? How do we make systems engineers think of security as a core function? How do we ensure that decision-makers consider cybersecurity as part of their leadership role? How do we build the trust relationships required to make systemic defenses scalable? More broadly, how does one develop a culture of cybersecurity?

Broadening the Discussion: Several participants noted that the workshop discussions did not link cybersecurity with the protection of physical infrastructure, though the two are interdependent. Foresman observed that while the intellectual depth of the cybersecurity discussion has improved greatly over time, the human mind is designed to approach problems individually. Intellectually, workshop participants tended to compartmentalize the discussion, focusing on cyber. Future discussions should consider the question of cybersecurity more broadly as it relates to physical and infrastructure security.

The Mission Statement: As the session concluded, the group articulated a mission statement. What we need going forward, it was determined, is a consolidated assessment of security standards that relates to critical infrastructure, in order to identify the capabilities and limitations of that infrastructure and prioritize the resources directed to those systems. And we must be able to do that in an all-threats, all-hazards environment.

Day One Keynote: Robert Carey, Deputy Chief Information Officer, U.S. Dept. of Defense

Robert Carey, Deputy CIO at the U.S. Department of Defense, described the challenges of securing a complex system of systems with components in hotspots throughout the world.

Key Points:

Complex System of Systems: The DOD's cyber assets include 10,000 networks running 25,000 applications, and 1,000 data centers. Many of these run in remote war zones or on ships at sea with only satellite connectivity. An aircraft carrier, for example, has less bandwidth than a typical home cable ISP.

Broad Universe of Threats: DOD networks face a phalanx of threats, ranging from rogue hackers drawn to state-sponsored espionage. The internal threat is also substantial. [The Wikileaks affair, in which a U.S. Army private copied more than 700,000 U.S. government documents from closed government networks onto a CD-RW labeled "Lady Gaga," is the most glaring example.]

Need for Decision-support Tools: The DOD has access to every cybersecurity tool on the market and the capacity to develop bespoke solutions, yet lacks the decision-support tools to choose the best products available for a given need. The need to develop for scientifically validated security metrics was an ongoing theme throughout the workshop.

Balancing Access and Security: DOD decision-makers demand functional performance and require access to network data from anywhere in the system, often under the most trying conditions. The challenge for DOD cyber professionals is to balance that degree of access with appropriate security.

Isolation is Not the Answer: Though many DOD systems are on closed networks, it is not feasible to isolate all or even most DOD activities from the Internet. The military supply chain relies heavily on private-sector companies, for example.

Renewed Commitment: In May 2010, DOD created the U.S. Cyber Command in Fort Meade, Md., under four-star Army General Keith Alexander.

Wednesday Morning Keynote: 20+ Years of Cyber (in)Security: What We've Seen, What We've Learned, What We Might Do

Richard Pethia, Director of the CERT Program at Carnegie Mellon University's Software Engineering Institute

Richard Pethia, Director of the CERT Program at Carnegie Mellon University's Software Engineering Institute, opened the workshop's second-day panel with an overview of cybersecurity breaches reaching back more than 20 years. Pethia enumerated the threat evolution, beginning with the internet worm in 1988; *Newsday* and Citibank hacks in 1994; and widespread attacks for profit by organized crime networks beginning around 2000. By 2007, he said, we had seen the opening salvos of state-sponsored cyberwar. Technical and design data relating to the Joint Strike Fighter (JSF) program was stolen from the computer system of a major defense contractor—an event that led to the establishment of the DOD Cybercrime Center. And the fact that the Russian invasion of Georgia in 2008 was preceded by a Distributed Denial of Service (DDoS) assault of Georgian computer networks suggests that cyber attacks will factor into future conflicts.

The Adversary is Getting Better: There has been a steady escalation in the sophistication of attack technology. Adversaries know how to attack our systems, they are increasingly automating those attacks, and they are engineering attacks that are more and more sophisticated in terms of hitting their targets.

The Air Gap is Gone: The Stuxnet worm, which was able to penetrate industrial control systems thought to be isolated from the Internet, is a case in point. A very well-engineered piece of malware discovered in July 2010, Stuxnet infiltrated Internet-enabled machines and was then passed to isolated industrial-control systems via USB port.

Change is the One Constant: The evolution of cyber threats tells us that change is the one thing that remains constant, and that vulnerabilities—though they may not always be the same--persist over time. We have seen an increase in cyber-espionage, and adversary tradecraft is becoming more sophisticated.

Complacency is a Risk Factor: Even as attack technology continues to evolve rapidly, users of computer systems are reluctant to accept compromises in performance. For decision-makers, functionality and connectedness often trumps security.

Ecosystem Approach: CERT collects about 8,000 new malware samples every day, of which only about 60 percent can be detected by the currently available antivirus programs. The solution therefore is to treat security as a first-class system function. Pethia advocates an ecosystem approach to cybersecurity encompassing human factors, economic factors, and the flexibility to respond to unexpected challenges.

Luncheon Speaker: Legal and Security Issues in Cloud Computing

Mark Rasch, Director, CyberSecurity and Privacy Consulting, CSC

Technology attorney Mark Rasch gave a memorable speech on the legal landscape surrounding cloud cybersecurity. The laws pertaining to cybersecurity are based on precedents from the analog age, with potentially disastrous implications for privacy and data security in the cloud.

Key Points:

The Answer Is, ‘It Depends:’ The law applies doctrine and concepts from the real world to cloud computing by analogy. The law that applies to a given legal situation therefore depends on which analogy an attorney chooses. The particular law that an attorney chooses depends on who his client is. For that reason, Rasch quipped that whenever anyone asks a legal question, the answer is “it depends.”

Little Protection Under the Law: Computer users care about protecting information—its confidentiality, availability, integrity. Yet the law is designed to protect physical property. It does not do a very good job of protecting information. For this reason, many early computer crimes were prosecuted as theft of electricity.

Search and Seizure: If the government has a search warrant for tax records stored in a filing cabinet, a police officer will search the cabinet, take the records, and leave everything else. But if those same records are on a computer, every document on that computer is subject to seizure. And, if the tax records are stored in the cloud, every document belonging to every user of that particular cloud is potentially subject to seizure.

Blame Barry Bonds: Two cases establish this precedent. In the first, a user on a cloud provider was suspected of criminal activity. The government, acting on a search warrant, seized the cloud’s servers and in the process shut down the network. The government had seized not only the information belonging to the suspected criminal, but that of every cloud user.

In the second, the government subpoenaed drug-testing results for 10 Major League baseball players who were among hundreds of players tested anonymously under an agreement between the league and the players’ union. The laboratory that held the records objected, and the court ruled in the lab’s favor. However, at the same time the court was making this ruling, the government obtained a search warrant and seized all the computers in the lab. On those computers were the records of the 10 players named in the original subpoena, as well as hundreds of other baseball players and thousands of other athletes. The government took the position that because the records were contained on a mass storage device, the government could use them in court—the original 10 and all the others—under what’s called the “plain view” doctrine.

Taken together, these two cases mean that suspected criminal activity by any cloud user makes all users of that cloud subject to search. If anyone on the cloud is suspected of criminal activity, your records are potentially at risk.

Cloud Security is at the Data Level: In pure cloud computing, in a multi-tenant environment, with everything being hosted by a third party, all the security has to be at the data level. In that case, concluded Rasch, encryption is your friend.

Dinner Presentation: The 2010 Verizon Data Breach Investigations Report

Marcus Sachs, Vice President for National Security Policy, Verizon

Marcus Sachs gave a dinner presentation on the 2010 Verizon Breach Report. The document is the latest in a series of empirical reports on adversary activity. This year the sample is much broader, thanks to the addition of data collected by the U.S. Secret Service. With the addition of Verizon's 2009 caseload and the Secret Service data, the Verizon breach series now spans six years, more than 900 documented breaches, and more than 900 million compromised records. The additional data served to validate the findings of earlier reports. The 2010 report revealed new attack trends, helped to define the scale of the problem, and served to frame much of the ensuing discussion in the workshop.

Key Points:

Detection is Abysmal: Only 11 percent of breaches are detected within minutes or hours of compromise. Detection is more likely to take days (22 percent), weeks (24 percent) or months (37 percent), and fully 7 percent of breaches take more than a year to detect. The detection to containment interval is equally bad: 13 percent within minutes or hours; 32 percent within days, 24 percent in weeks, 29 percent in months, and 3 percent in a year or more.

Easy Targets: 98 percent of all data breached came from servers; 85 percent of attacks were not considered highly difficult; and 86 percent of victims had evidence of the breach in their log files. Despite the log evidence, 61 percent of breaches were discovered by a third party.

(Mostly) Easy Fixes: 96 percent of breaches were avoidable through simple or intermediate controls, and 79 percent of victims subject to PCI DSS had not achieved compliance.

Insider Threat: Almost half (48 percent) of the breaches investigated by Verizon and the Secret Service in 2009 were attributed to insiders. This represents a 26 percent increase, possibly attributable to the type of crime the Secret Service investigates.

Insider Tactics: 48 percent of breaches involved privilege misuse (up 26 percent), a trend that is related to the increased proportion of insiders. Hacking (40 percent) and malware (38 percent) round out the top three, and were responsible for more than 95 percent of all data compromised. Breaches involving social tactics nearly doubled to 28 percent (up 16 percent).

Financial Services the Biggest Target: Financial services companies were the target of 33 percent of attacks and 94 percent of records lost. Hospitality (23 percent) and retail (15 percent) were second and third by attack volume. Government was the target of 4 percent of attacks.

List of Acronyms

CATE	Coordination Awareness, Training and Education
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CTO	Chief Technology Officer
CISSP	Certified Information Systems Security Professional
CERT acronym	A collaborative network security organization; not an acronym
CERT/CC	CERT Coordination Center
DCCI	Defense Cyber Crimes Institute
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security.
DOD	Department of Defense
FBI	Federal Bureau of Investigation
I3P	Institute for Information Infrastructure Protection
IBM	International Business Machines Corporation
INCOSE	International Council on Systems Engineering
ISAC	Information Sharing and Analysis Center
JSF	Joint Strike Fighter
MITRE	MITRE Corporation; not an acronym
NASA	National Aeronautics and Space Administration
NCCIC	National Cybersecurity Communications Integration Center
NSA	National Security Agency

PCIS	Partnership for Critical Infrastructure Security
SANS	The SysAdmin, Audit, Network, Security Institute
USSS	United States Secret Service