I3P Workshop Report

Workforce Development: Understanding the Demand

Sponsored by
The Institute for Information Infrastructure Protection (I3P)

Co-chaired by
Seymour E. Goodman, Shari Lawrence Pfleeger,
Ronald Dodge, and Thomas Longstaff

Georgia Tech Hotel and Conference Center – Atlanta, Georgia
April 27-28, 2011
# Table of Contents

Acknowledgments.................................................................................................................. 3  
Executive Summary................................................................................................................ 4  
Why a Workshop on Workforce Development? ..................................................................... 6  
The Workshop Process............................................................................................................ 7  
Characterizing the National Demand: A keynote talk by Roberta G. Stempfley.................. 8  
Breakout Session One: Understanding Government Demand .............................................. 11  
  Demand in State and Local Government.......................................................................... 11  
  Demand in the Federal Government................................................................................. 12  
  International Demand........................................................................................................ 12  
An Enterprise Perspective on the Security Workforce: A keynote talk by William G. Horne 14  
Breakout Session Two: Assessing Industry Demand.............................................................. 16  
  Demand in Small Business............................................................................................... 16  
  Demand in Critical Infrastructure...................................................................................... 16  
  Demand in the Supply Chain............................................................................................ 17  
Achieving An Integrated Cyber Security Workforce: A keynote talk by Stephen J. Lukasik .. 19  
Breakout Session Three: Security and Organization Structure ........................................... 22  
  How Security is Infused in Non-Security Jobs.................................................................. 22  
  How Security Aligns with Organizational Business and Culture .................................... 22  
  How Demand Is Appropriately Expressed to Human Resources ...................................... 23  
Key Insights and Recommendations ...................................................................................... 25
Acknowledgments

The organizers thank the workshop presenters and participants for their time, advice, candor and leadership in the field of cyber security. They also wish to express their gratitude to the Department of Homeland Security for its support of this workshop and for its continuing commitment to securing the nation’s information infrastructure.

The material in this report 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.

For more information about this workshop or the Institute for Information Infrastructure Protection, please contact Martha Austin (Martha.F.Austin@dartmouth.edu) or Shari Lawrence Pfleeger (Shari.L.Pfleeger@dartmouth.edu)
Executive Summary

Securing the information technology infrastructure requires a large and diverse workforce with a wide range of skills, the specific composition of which has not yet been well defined. To gain a better understanding of the demand for cyber security workers in government and private industry, the Institute for Information Infrastructure Protection (I3P) sponsored the workshop “Workforce Development: Understanding the Demand.” The event brought together forty people representing government agencies, private companies and academic institutions on April 27 and 28, 2011, at the Georgia Tech Hotel and Conference Center in Atlanta, Georgia.

Developing an effective cyber security workforce is a difficult undertaking. The threat is rapidly expanding, as is the importance of information technology to our economy and daily lives. As the use of computing devices continues to grow, people and organizations are becoming more dependent on information technology for their health and welfare. Increasing reliance on information technology creates a growing number of vulnerabilities that have the potential to compromise, destroy or block access to essential functions and data. New threats emerge as systems and operating norms continue to evolve. For example, cloud and mobile computing offer enormous potential benefits, yet each presents daunting new security vulnerabilities.

Cyber security jobs are by their nature constantly evolving to keep pace with innovation and change. This dynamism creates difficulty for everyone in the talent supply chain, from educators to line managers. One workshop participant neatly summed up the pace of change by observing that none of the cyber security jobs he has held in the last 20 years existed when he started his career.

Because specific job roles will shift with the advent of new threats and new technologies, participants agreed that competency in core skills is essential. These capabilities include both quantitative skills such as engineering, mathematics and computer science, as well as behavioral skills such as management, communication and the ability to think creatively.

Thus, the demand for cyber security expertise cannot easily be described with a uniform skill profile. Rather, needed expertise encompasses an ecosystem of complementary knowledge, skills and abilities. A health care analogy was frequently employed to describe the variety of needed cyber security roles. Just as health care professionals include brain surgeons and family practitioners, research scientists and paramedics, administrators and nurses, cyber security demands a workforce with a similarly diverse set of skills and responsibilities. In both fields, if any of the critical roles is lacking, the system could not function properly. And in both domains, effectiveness is a team effort: people with widely varied skill sets work together to counter threats that they would be unable to identify or defeat alone.

Training such a diverse workforce requires contributions from a range of academic and training institutions, including universities, community colleges, trade schools and
military occupational specialties. Practical experience is another essential component of workforce development, so there is a need for continued training and mentorship beyond the academic setting. Cyber security must be infused into many different jobs, a substantial proportion of which may not require a computer science major or even a college degree. To the extent that organizations can define the role of cyber security in every employee’s job duties, a comprehensive program can ensure that all workers have the appropriate education, training and tools to perform their jobs in an effective and security-conscious manner.

A taxonomy of cyber security jobs and associated skills would be a valuable tool enabling employers and educators to define and meet the demand. A number of related efforts are underway, but the results as yet are incomplete and not easily applied across the entire cyber security workforce. The workshop identified the completion of a comprehensive and flexible taxonomy as an action priority for enabling better articulation of what is needed in which contexts.

Once the demand is articulated, it will be important for all constituents to be able to predict where the need is most severe and, eventually, how well it is being met. Workshop participants agreed that a scientific basis for projecting, classifying and measuring the contribution of cyber security is lacking. A general paucity of representative, credible data about the nature and magnitude of cyber security problems complicates the ability to project current and future need. Moreover, for security and liability reasons, organizations are often loath to share data about security breaches and near failures. Demonstrating the need for cyber security to decision-makers in terms they understand is hampered by a lack of evaluative tools; without them, organizational executives cannot easily weigh the benefits of investing in other initiatives (e.g. new products or services, new staff capabilities) with security investments. As a result, cyber security is disadvantaged in the competition for resources because it is rarely seen as contributing to an organization's core mission; it consumes resources without visibly adding to the bottom line.

Remedies used in other settings may be useful in addressing cyber security demand. For instance, regulation could encourage organizations to pay careful attention to security issues, much as HIPAA and the Sarbanes-Oxley Act have shaped cyber security thinking in the health care and public accounting industries, respectively. Regulation sometimes changes the nature and magnitude of resourcing, and in this case it could shift focus to compliance; additional steps would be needed to ensure that compliances results in effective security.
Why a Workshop on Workforce Development?

In our information-based economy, many organizations have information technology (IT) at the core of their enterprise. This universe of “IT security customers” includes all levels of government, defense and critical infrastructure, as well as industries as varied as manufacturing, retail and financial services. Each of these users has discrete needs for cyber security professionals and capabilities. Collectively, these users represent the cyber security workforce demand. The workshop sought to identify common themes, discuss strategies to better quantify and categorize the workforce development demand, and chart a course toward a more systemic approach to meeting this demand.

The workshop brought together Information Technology managers, educators, and thought-leaders from government, private industry and academia in an effort to define the evolving cyber-security workforce requirements from a demand-based perspective. The workshop’s 40 participants share common interests in information security, critical infrastructure protection, education and workforce development.

The workshop participants shared their concrete workforce needs in order to collectively develop a more complete and nuanced understanding of the demand. Among the workshop’s goals were to:

- Develop a more complete understanding of employer demand for cyber security skills so that employers and educators can work together to meet the demand.
- Facilitate communication and cooperation between cyber security workforce customers and providers so that supply will more closely track demand.
- Recognize emerging trends in cyber security workforce demand so that training programs can be developed or enhanced to provide new capabilities when they are needed.
- Provide a framework for needed research and action in the future.
The Workshop Process

The workshop took place April 27 and 28, 2011, at the Georgia Tech Hotel and Conference Center in Atlanta, Georgia. It was sponsored by the Institute for Information Infrastructure Protection (I3P), a research consortium managed by Dartmouth College, and supported with funding from the Department of Homeland Security’s National Cyber Security Division.

The workshop featured three keynote talks by experts in government, private enterprise, and academia. After each keynote, participants joined one of three breakout groups to discuss more focused questions related to government demand, industry demand, and workforce integration. Following each of the breakout periods, participants convened to discuss the findings of each group, and to engage in probing, dynamic discussions.

The workshop concluded with a group discussion of key findings. The participants also suggested several ways for research and practice that will encourage the workforce supply to meet a clearly-defined demand. Below is a summary of the workshop agenda.

Opening Remarks: Seymour E. Goodman, Georgia Institute of Technology

First Keynote: Roberta G. Stempfley, Department of Homeland Security

First Breakout Period: Government Demand (state and local; federal; and international).

Second Keynote: William G. Horne, Hewlett Packard

Second Breakout Period: Industry Demand (small business; critical infrastructure; and the supply chain).

Third Keynote: Stephen J. Lukasik, Georgia Institute of Technology

Third Breakout Period: Workforce Integration (infusing a security role in non-security jobs; aligning security with organizational culture; and communicating demand to human relations staff).

Workshop Summary Discussion: Facilitated by Shari Lawrence Pfleeger
Characterizing the National Demand: A keynote talk by Roberta G. Stempfley
Deputy Assistant Secretary, Cybersecurity and Communications for the Department of Homeland Security, and recent Director of the National Cybersecurity Division, Department of Homeland Security

In her role as director of the National Cyber Security Division (NCSD), Roberta Stempley oversaw programs aimed at improving IT security across the federal government. Her keynote talk outlined some of the factors that influence development of the cyber security workforce, including constrained government budgets, rapidly escalating demand, and the need for security professionals with a mix of quantitative and behavioral skills.

Key Points:

Cyber Security is Not Mission-Specific: Information technology is rarely the mission or core function of an organization, making it difficult for organizational managers to obtain needed cyber security resources, particularly in a budget-constrained environment. “It’s really, really hard for DHS to make an argument for funding something that appears to take money away from providing very important citizen service,” Stempfley said. Communicating the value of effective security is difficult. At the executive level, the need for cyber security often isn’t recognized until security is breached. For these reasons, cyber security should always be considered in the context of the mission.

Money Matters: Resourcing remains a tremendous challenge. Can we afford the necessary level of IT security? The question has no answer, as nobody knows how secure is secure enough. Trends in hiring suggest increasing demand for cyber security. However, needs differ among large, mid-size and micro agencies. One thing that is clear is that one cyber security workforce solution does not fit all.

A Trend Away From Direct Control: Cost savings make cloud computing extremely attractive to management, despite considerable security concerns. Both industry and government are therefore rapidly embracing distributed computing, including substantial use of cloud products and services. Similarly, outsourcing cyber security roles to outside contractors can yield attractive cost savings, particularly in smaller agencies that lack in-house capabilities. The result of both these cost-driven trends is a reduction in direct agency control of cyber security processes and personnel. The people who manage contract security staff must be as knowledgeable as those they supervise but, as Stempfley noted, as government agencies rely more on outsourcing, the knowledge of the responsible decision-makers tends to degrade over time. It is imperative to maintain that knowledge level so that managers understand the nature and ramifications of the decisions they make.

The Data Deficit: Credible data that will allow decision-makers to quantify and classify demand for cyber security workers are only now becoming available in some sectors of IT security. But the data deficit is complex. Much of the nation’s critical infrastructure is owned by private enterprise. As part of its mission, the NCSD provides technical assistance to both
private and public critical infrastructure users and providers, to help them understand their needs and the remedies available to them. Recently, NCSD began receiving data about how each federal agency measures against a set of cyber security standards. This data set helps NCSD estimate how much technical assistance to provide to help the agency improve its cyber security posture relative to the standards. In ways such as this one, the nation could benefit from access to better data about the rapidly growing and shifting set of cyber security requirements and the activities that address them.

**A Need for Exceptional People:** Effective cyber security requires staff and users with specific technical skills, but it also demands people who can think on their feet. The nation needs people who use intuition, who can assert and prove, and whose thinking is not constrained only to systematic, step-by-step processes. “There aren't a large number of people who can make that leap,” Stempfley said. “Those who can are phenomenally powerful as they go forward in their careers.” Thus, the cyber security demand is not purely a question of training technicians; it also involves building well-rounded professionals who can make security decisions in the context of their organization’s mission and resources. At its core, IT security is about people in a distributed environment making independent decisions based on a common understanding of technological capabilities and needs. Achieving this balance in an organization is a complicated problem.

**A Soaring Demand Curve:** Keeping pace with skyrocketing demands for cyber security workers is a daunting challenge. Stempfley’s NCSD has grown from 38 people to more than 200 in the last three years. Managing such rapid growth is a tremendous challenge, particularly since many agencies are vying to attract enough qualified people, and each new person faces a steep learning curve in how the organization works. Stempfley has had to reduce her personnel requests to maintain a manageable growth rate.

**Security is Market-driven:** Consumers often embrace new technologies with little regard for information security consequences. Stempfley used the example of Ford and the Apple iPod to illustrate this point. The automaker produces 2 million cars annually; Apple sells 12 million iPods in the same period. Ford executives therefore say they have no choice but to put iPod connectivity in every car. Consumers demand it, so Ford provides it. The Apple technology is integrated into Ford automobiles, presenting potential new threats to functions and features. Distributed computing and smart phones are two more worrisome examples. In similar ways, new technologies and their incorporation into existing products and systems are rapidly adding to the threat profile.

**Make Security Central:** One participant asserted that the effectiveness of a cyber security regime is relative to its position on the organizational chart. If it's on the periphery and not seen as essential to the organizational mission, its security will be under-resourced and poorly integrated. If it is central to the organizational structure and mission, it is much more likely to be effective. Cyber security therefore should be “baked into” business and government systems; security cannot be seen merely as a compliance problem. Aviation, a technologically advanced field that has achieved an excellent safety record, provides a useful analogy. Aviation safety is not solely the province of pilots and aeronautical
engineers. Mechanics, air traffic control staff, airport operations officials, flight attendants, gate agents and many others contribute to aviation safety.

The Role of Regulation: One participant, a retired military aviator, noted that aviation safety had improved dramatically as a result of regulation; safety plays a role in licensing, mandatory inspection schedules, and commonality of procedures and controls. Regulation has spurred cultural shifts in other industries as well. For example, the Occupational Safety and Health Act has had a profound effect on workplace safety; the Sarbanes-Oxley Act has resulted in more rigorous accounting practices; and the Health Information Portability and Accountability Act (HIPAA) has made information security a priority in the medical field. Such regulation can make managers more accountable for failures, including regulatory lapses. Greater regulatory accountability could therefore create an incentive for decision-makers to devote more resources to cyber security. However, there is always the risk that emphasis could shift to compliance from effective security.
Breakout Session One: Understanding Government Demand

The workshop participants divided into three groups to discuss the demand for cyber security professionals from state and local governments, the federal government, and international government. Following the one-hour breakout sessions, the full group reconvened to hear and discuss the findings of each breakout.

Demand in State and Local Government

Small Government is a Big Player: Taken as a whole, state and local governments in the United States employ 6.3 people for every person employed by the federal government, and their combined payrolls are 4.6 times larger than the federal government’s. According to March 2009 U.S. Census Bureau data, the federal government employs 2.8 million people, with a monthly payroll of $15.1 billion. State governments employ 3.2 million, with a $19.4 billion payroll. Local governments comprise by far the largest segment, with 14.5 million employees and a monthly payroll of $50.7 billion. It follows that state and local governments are a significant driver of demand.

One Size Does Not Fit All: State and local governments vary tremendously in size, ranging from departments with just a handful of staffers to organizations that rival those on the federal level. Cyber security staffing needs are in part determined or constrained by size. For example, the North Dakota Bureau of Investigation consists of seven people; it doesn’t employ an IT person, let alone a cyber security specialist. By contrast, the New York City Police Department has more than 38,000 uniformed officers, including a dedicated cyber crimes squad.

Resources are Limited: Budgets at the state and local level are more constrained than those in federal agencies. Unlike the federal government, many state and local governments are prohibited by statute from operating at a deficit. This restriction means that no matter how great the need, cyber security requirements sometimes go unaddressed. In general, state and local agencies pay less than their federal counterparts for equivalent jobs. This wage disparity makes it more difficult to recruit top talent.

All Politics are Local: State and local government workforces are rooted in the local community. They are subjected to real-time political pressures, such as residents complaining at City Hall or the Statehouse about a particular lack of service. Rarely do constituents complain to lawmakers about cyber vulnerabilities. Local political demands can potentially skew funding priorities, giving short shrift to cyber security needs.

The Pervasive Data Shortage: State and local government cyber security demand is difficult to measure. Anecdotally, it seems as though local needs vary widely, and expedient solutions are determined on a case-by-case, locally-developed basis. State and local governments would benefit greatly from tools to help them identify their cyber security needs. Despite their large aggregate size and budgets, state and local governments lack both the tools and coordination required to wield commensurate influence on demand.
Demand in the Federal Government

Civilian Agencies Will Drive Demand: Federal government cyber security needs differ greatly among agencies. Agencies that deal with security, such as DOD, DHS and the intelligence community, have been the principal demand-drivers to date. As IT becomes more ubiquitous, however, civilian agencies may account for more of the demand. They also are likely to create a more varied demand, because of the wide variation in agency missions.

Top Management Still Doesn’t “Get It”: Many decision makers in the federal government still don’t recognize the potential cost of ignoring cyber security issues. Just as in the private sector, management in federal agencies is frequently unaware of the potential mission threats posed by cyber security issues. Communicating the business case to top management—demonstrating that investing in security can pay dividends or avoid significant costs—is therefore an essential piece of the demand equation. In the private sector, a catastrophic breach can cause a company to fail. A federal agency is unlikely to go out of business, but a damaging breach will hit government managers where it hurts most—in the form of lost turf, reputation and budget. If their impact is made public, breaches can also cause embarrassment and erode public trust.

An Uncertain Science: Currently, there is no scientifically validated method for forecasting the demand for cyber security professionals. In the federal sphere, as elsewhere, the cyber security threats are continually evolving. The breakout participants agreed that a credible method of projecting future demand is needed. This method would include not only the evolving threats but also ways to quantify the business case for investing in security to defend against these threats and mitigate their effects.

Standardization is in the Works: The National Initiative for Cyber Security Education (NICE), a multi-agency project of the federal government, is actively working on tools to address the demand projection and business-case issues identified above. Specifically, the Office of Personnel Management is leading a workforce development track within NICE.

International Demand

Need for Multilateral Cooperation: Cultural, legal and jurisdictional differences complicate the implementation of cyber security across national borders. Creation of common ground for cooperation would be valuable, facilitating discussion, analysis and coordinated action. The problem is too large and complex to be effectively addressed using bilateral agreements between nations. This complexity suggests a need for an international cyber security organization that builds on existing institutions—a World Health Organization for cyber security. The United Nations or the International Telecommunications Union may provide an avenue for such an international framework.

Assessing International Demand: Significant demand for cyber security services is centered in developed economies, such as the United States, Europe and Japan. Demand also is growing rapidly in developing information economies, such as Brazil, China, India, and other parts of Asia. Less-developed countries account for less demand but offer unique
challenges. For example, in much of Africa and Asia, banking services are increasingly being provided via messaging on cellular networks.

**Demand is Locally Driven:** Each country is unique, and its demand for cyber security—as well as its willingness to cooperate with international cyber security initiatives—will depend on local culture, laws, and economic factors. Grass-roots phenomena such as the use of information technology across political boundaries (e.g. the role of social networking in the Arab Spring) also drive specific demands for cyber security capabilities. The adaptation of new technologies also shapes demand (e.g. Cloud computing, and President Obama’s reported dedication to his Blackberry, manufactured by a Canadian company). In the developing world, entire generations of information technologies can be leapfrogged; for instance, some countries or areas that never had a landline telephone infrastructure now experience the proliferation of mobile phones.

**Local Laws and Culture Shape Demand:** Compliance with varying privacy, labor laws, and audit requirements has an enormous influence on the need for cyber security capabilities in each jurisdiction. Scandals and public failures can push demand and regulatory priorities. In some countries, direct government control of the economy is a significant factor affecting demand. Currently, many professional certifications do not cross international borders. For example, U.S. certifications are not applicable to Japan, where a member of the workforce often rotates through job responsibilities within a company rather than remaining in a specialty.

**National Security Needs Influence Demand:** “How do you support global security at the same time that every country sees every other country as a potential problem?” one participant asked. Examples of international risks abound. For instance, faced with a local supply and demand mismatch, Abu Dhabi imports much of the IT security work force for its enormous energy infrastructure, creating significant national security liabilities. In Israel, all critical infrastructure is regulated by the national government, creating demand for strong cyber security capabilities. These examples suggest that it may be easier for a small country to adapt to demand than for a large country. On the other hand, large countries may be able to do more precisely because they are large.
An Enterprise Perspective on the Security Workforce: A keynote talk by William G. Horne

Research Manager, Systems Security Lab, Hewlett-Packard

Bill Horne spoke about the cyber security workforce from the perspective of a large multinational firm with an extensive technology portfolio. Although the security experiences at Hewlett-Packard (HP) may not translate to all companies, they are indicative of many of the challenges faced by most enterprises. HP is the largest technology provider in the world, consisting of 325,000 employees operating in 170 countries. It faces security workforce development challenges similar to those at many large technology companies: a competitive recruiting and retention environment; the lack of a cyber security skills taxonomy, and an uncertain business environment.

Key Points:

A Need for a Common Taxonomy: Currently, no universal system exists to classify cyber security skill sets. HP employs 325,000 people, including a large and diverse cyber security workforce. However, Horne said, “there’s no database I can query to find out how many of those people know government and risk management and how many people know incident response.” Such a taxonomy is not even available for purchase. The federal government is building a functional role matrix that has experienced notable success, but the matrix has had limited usefulness to industry. Something finer-grained than the status quo in industry—which often consists of employees clicking an “I have security” check box—is needed to effectively match the work force with jobs.

Competition for Cyber Security Recruits: HP views its security workforce as a strategic asset. Its annual report states that HP’s ability to attract, retain, and motivate employees is key to the company’s success. This capability is true of other successful organizations as well, so HP must compete with government, other established companies, and startups to attract skilled cyber security workers. White-hat hackers skilled at ferreting out vulnerabilities are particularly difficult to recruit due to intense competition and a sometimes difficult fit in the corporate environment. Recruitment by acquisition is one solution. HP recently bought 3Com, which has the market-leading intrusion detection system, Tipping Point, in its portfolio. A Tipping Point subsidiary, DV Labs, includes “a bunch of guys in black turtleneck shirts who figure out how to break things and how to hack them,” Horne said. In other words, HP was able to acquire a complete team full of hard-to-recruit talent, adding considerable depth to its security capability.

Uncertainty Hinders Planning and Retention: The uncertainty inherent in the contracting process makes it difficult for contract-oriented companies such as HP to project staffing needs in advance. HP typically bids for dozens of contracts at any given time, including some that are very large. Winning a $100 million contract generates an immediate need for 500 new staff, many with specialized skill sets. Filling those positions can be an extraordinarily difficult task. Uncertainty trickles down to the employee level as well. Staff
who are not assigned to a contract, or who are assigned to a contract that is about to expire, naturally become nervous about their job security. They are more likely to look for work outside HP. This uncertainty makes retention of key employees more difficult. Employee burnout is also a factor, because the rigors of crisis response—work that is often both intense and tedious tasks, such as reviewing data logs—erode staff morale. HP is developing a mathematical model to better forecast workforce demand.

**Security is an Ecosystem:** Cyber security encompasses a broad and rapidly expanding group of capabilities, and it involves supporting activities in nearly every facet of the economy. In this respect, security is much like health care. There’s more to medicine than hiring the best doctors and nurses; an effective health care system requires a broad diversity of roles: EMTs, medical equipment providers, hospital administrators, pharmaceutical research and manufacturing, insurance services. Similarly, cyber security requires an ecosystem of skills, both general and specialized, among them computer scientists, programmers, forensic analysts, cryptographers, white-hat hackers, risk-management specialists. A Venn diagram of all these necessary skills would have very little overlap.

**Degrees of Security Responsibility:** HP expects everyone in the organization to have some level of security awareness. The spectrum ranges from staffers, whose only exposure is a yearly course to raise awareness, to full-time security professionals, who deal with security every day. Of the 6,548 job openings advertised by HP at the time of the workshop, 22 percent have the keyword “security” in the job descriptions. The majority of these openings are for security professionals, such as IT administrators and people with specific security expertise.

**Need to Share Versus Liability:** Companies and government agencies that work with technology and security collects vast quantities of threat information. However, they are reluctant to share these data, particularly when they relate to a successful cyber attack: data’s owners may have severe liabilities related to the security failure. In many cases, compromised data themselves may be privileged or sensitive. Cultivating and maintaining trust within and between organizations can in some cases mitigate this problem. Within HP, building relationships has empowered generous data sharing.

**Security is Not Yet a Science:** The inability to share data hampers development of a true security science. Security-related experiments aren’t reproducible in the same sense as physics or chemistry. But there is a need to develop means for sharing specific, real-world security data to support the design and building of better defenses to evolving threats.
**Breakout Session Two: Assessing Industry Demand**

The workshop divided into three groups to discuss the demand for cyber security professionals from small business, to support critical infrastructure, and in the supply chain. Following the one-hour breakout sessions, the full group reconvened to hear and discuss the findings of each breakout.

**Demand in Small Business**

**Small Business, Big Definition:** The term “small business” describes a broad range of businesses. According to the U.S. Small Business Association, the term includes everything from sole proprietorships to privately owned manufacturing firms with as many as 1,500 employees. Most of the group’s discussion was centered on businesses of between five and 50 employees, operating in fields such as medicine, law, financial services and information security. Though it’s difficult to generalize across such a range, we can say with very few exceptions that a single small business cannot by itself drive demand in the way that a large corporation or government agency can.

**Small Businesses are Customers:** Small businesses typically rely on IT systems developed by large companies, and in most cases they depend on the security functions built in to the computers and software they purchase from large businesses. Such built-in security tends to be poor. As customers of IT hardware, software and service providers, small business is in a position to demand better security, creating an indirect demand for security engineers, programmers and the like. The same holds for cyber support services. Small businesses that rely on “Geek Squad” contractors for IT support are in a position to demand that those technicians be versed in security.

**Lack of Dedicated Resources:** Small businesses, however varied and broad in function, rarely enjoy dedicated IT resources, let alone specialized cyber security resources. IT skills are often a subset of another job. For example, the task of managing the office computer system will fall to an administrative assistant or a medical billing agent. In many small businesses, basic IT functionality takes higher priority than security.

**Make Integrity Pay:** Currently there is insufficient economic incentive for IT systems developers to build secure systems. If sensitive medical records are stolen from a small medical practice that relies on vulnerable software, the developer of that software is not usually held liable. Thus, there is little incentive for the developer to incur the added cost of building more secure software. Legislation or enforcement of legal liability may be required to drive security improvement.

**Demand in Critical Infrastructure**

**Narrowing the Scope:** To focus its discussion, the participants used as an example an electric power company, an essential part of critical infrastructure. The hypothetical power company has classic IT systems, including control systems. Management is IT-savvy, and cyber security is the responsibility of professionals trained and responsible for that role. The principal focus is not on information security, as is often the case in government or the
service industry; rather, it is literally about keeping the lights on. The emphasis is on profitability and domain engineering. The corporate executive is briefed daily on market performance and is focused on the creation of shareholder value, not cyber threats.

**Service Recovery Focus:** Because the money allocated to maintain services is finite, and cost/benefit analysis for IT security is unclear, service providers focus on recovery rather than incident prevention. As one participant said, “They don’t care what brings them down so long as they come back in a certain amount of time.” For example, following the Northeast Blackout of 2003, executives at First Energy allegedly said they didn’t care whether the failure had been caused by equipment failure or cyber attack; they cared only about restoring power.

**Regulation is a Dirty Word:** The participants engaged in a lively discussion on the issue of regulation. Some said that because these infrastructures are critical, it makes sense to legislate demand for better cyber security. Other participants strongly resisted additional regulation, due to its financial implications. In highly cost-sensitive industries, there is little room in the financial model to absorb new IT security costs.

**Complicated Culture:** Domain engineers and IT security professionals speak different languages and have different, highly specialized priorities. Culturally, completing essential business tasks takes priority, resulting in an imbalance of pay, prestige and power. Turnover among domain engineers provides an opportunity for better training and security awareness in a new generation of domain engineers. A 2009 study by the U.S. Power and Energy Engineering Workforce Collaborative found that by 2014, approximately 45 percent of engineers now working in electric utilities will be eligible for retirement or could leave engineering for other reasons.

**The Smart Grid:** The question of the “smart grid” generated a round of animated discussion, with some participants contending it offers an opportunity to “bake in” security, while others believe it presents new cyber vulnerabilities. If security can be integrated from the beginning, the smart grid has the potential to drive costs down in the entire enterprise. Making such a grid secure is a challenging task, demanding of significant resources. With the push to quickly deploy a smart grid, some participants were pessimistic that it will be well engineered from a cyber security standpoint.

**Demand in the Supply Chain**

**A Two-fold Discussion:** Participants discussed two aspects of supply chain demand: the supply chain of qualified cyber security workers, and the challenge of securing a supply chain from cyber attack.

**Academic and Practical Training:** Effective cyber security people are cultivated in a variety of ways, including academic training, military schools, and industry work experience. The most effective practitioners often result from a mix of these methods. Using an analogy from the medical profession, one participant noted that medical schools don’t
graduate brain surgeons. They produce physicians, some of whom later become brain surgeons through clinical training and practice. The same holds true in cyber security.

**A Variety of Paths:** Job functions in the cyber security field run the gamut from administrative to highly technical. As one participant noted, we need both engineers to design systems and equipment operators to run them. The venues for training are therefore equally varied. It is a mistake to focus solely on university computer science programs; trade schools, community colleges and the military are also important sources of initial training. Practical training likewise occurs in a variety of settings.

**The Cyber Operator:** The military integrates information management specialists, computer site specialists and communications specialists. Together with military intelligence, they form a multi-disciplinary work force. This integrated team model could be effective in non-military settings as well.

**Need for a Common Terminology:** In the supply chain as in other IT security dimensions, the lack of a common lexicon—for example, what it means to say an employee is “qualified”—hampers effective analysis, planning and workforce development.

**Opportunity in Crisis:** Major events, such as the 9/11 terrorist attack, create periods of heightened security awareness, resulting in opportunities to insert greater security controls into the supply chain. The participants wondered what major event would cause cyber security to be recognized as an imperative in the realms of financial services, critical infrastructure and national security.

**Cost is the Driver:** When organizations base decisions on cost, better—and thus more costly—security becomes a hard sell. In highly competitive industries, decision-makers often feel they cannot afford to pay for security, because it puts them at a competitive disadvantage with companies that focus solely on functionality or time-to-market. Nevertheless, building secure code is an attractive solution to some companies, because it is perceived to be less expensive than intervention or the certification of manufacturing facilities.

**Data Security:** If security controls were attached to the data, rather than to the system containing it, the focus of cyber security workforce development would change. However, data are used in ways the data creators may not have intended them, so it may be difficult to decide on appropriate security at the data level.
Achieving An Integrated Cyber Security Workforce: A keynote talk by Stephen J. Lukasik

Stephen J. Lukasik gave a keynote talk on how to develop an integrated cyber security workforce. He advocated a multi-disciplinary approach to cyber security, rejecting “Edisonian” thinking in favor of a methodology based on established sciences that study active agents.

Key Points:

We're a Long Way From an Integrated Security Workface: Today’s cyber security workforce, while competent in many ways, is not delivering the level of security the nation requires. James Lewis, Director of the Technology and Public Policy Program at the Center for Strategic and International Studies, articulated one aspect of the problem when he told an interviewer last year that “there is no correlation between the training cyber professionals receive and the job they have to do.” Demand is best measured as what’s necessary to deliver the desired result. The skill levels of the cyber security workforce are relevant only to the extent the workforce is tasked with the “right” jobs.

The Cost of Security: In principle, an organization can have any level of security that it is willing to pay for. Cyber security has implicit as well as explicit costs. The challenge for security advocates is to convince decision-makers that it is in their interest to pay for sufficient cyber security. To make this case, we must be able to measure the cost—and the value—of cyber security. “If, like potatoes, cyber security is sold by the pound, then one has to know what a pound of cyber security costs,” Lukasik said.

Problem Actors: Three types of people create cyber security risk: the overtly malicious, the knowledgeable but security-imprudent, and the uninformed who create vulnerabilities without knowing it. Malicious actors are the source of the problem; the others are enablers. There is a global criminal “service industry” devoted to exploiting cyber vulnerabilities. It rents botnets, sells zero-day exploits and stolen personal information. Fund transfers in this worldwide underground industry are conducted using a more secure analog of PayPal run by a Russian criminal syndicate.

A Global Playing Field with Escalating Consequences: Cyber security is a global problem. The threat exists in all legal jurisdictions. Some countries actively work to contain the problem; others contribute to it; and some are part of the landscape. While criminal activities like theft, fraud, spyware and privacy intrusions don’t rise to the level of existential concern, the threat of more damaging attacks is very real. The Stuxnet worm, widely believed to have been designed by U.S. or Israeli government actors to slow the Iranian nuclear weapons development effort, is itself something of a weapon of mass destruction. The malware serves as proof-of-concept that a cyber attack is capable of
disabling critical infrastructures, even if they are isolated from the internet. This example is a sobering development in the “cyber arms race.”

**Cyber Security is Not Exclusively a Technology Problem:** Defining cyber security as a technical problem only addresses about 50 percent of the problem, Lukasik said. Effective cyber security demands a mix of skills, including law, diplomacy, and management in addition to information technology. Lukasik referred to two study groups in which he had taken part, a National Research Council study of international enforcement, and a DARPA program addressing the problem of malicious insiders. In both cases, technologists comprised approximately 40 percent of the team.

**The Right Kind of Science:** The Department of Defense recently asked the JASON study group, an independent panel of scientists that advises U.S. government agencies, to assess whether there are “laws of nature” in cyberspace that can form the basis of scientific inquiry in the field of cyber security, and to determine which elements of scientific theory, experimentation, or practice the cyber security research community should borrow to make progress in the field. The panel’s answer was two-fold. First, cyber security should avoid “Edisonian” approaches seeking specific inventions that address one particular problem. Second, scientific domains in which there are active agents operating can provide especially relevant insights. The study group identified economics, meteorology, medicine, and agriculture. Lukasik said that he would also add psychology and game theory to that list.

**Barriers to Security Integration in Higher Education:** Universities are organized by academic discipline, which creates barriers to developing the integrated knowledge required of effective cyber security agents. Institutions have addressed this problem through the creation of interdisciplinary research and development centers, but in practice parochialism remains a significant barrier. Another approach has been to adopt the clinical practice model to address real-world problems that, by their nature, are interdisciplinary. Community colleges and trade schools are more receptive to the interdisciplinary approach because these institutions are heavily career-oriented, and careers are, by their nature, interdisciplinary. The rapid pace of technology necessitates continuing education and professionally administered licensing to maintain certification as done in medicine, law, and accounting.

**Software Hygiene Must Improve:** Cyber security would be more effective if the people specifying, writing, releasing, and licensing software committed fewer security blunders. The software maturity ratings and the subsequent system engineering maturity ratings established by the Carnegie Mellon Software Engineering Institute suggest a useful extension to security maturity ratings. Currently, software engineering is centered on the “doing” functionality, the command side of the “command-and-control” principle. The control side deserves more attention. An independent regime of cyber security audits, analogous to auditing protocols in the public accounting industry, would improve security and user confidence.
**Impetus for Positive Change:** Companies and governments have significant stakes in the trust of their constituents, the value of their financial assets and intellectual property, and their national security assets. Less explored is the role of users in calling for safety, security, and reliability in the cyber commons. Calling for action through social networks, and using users’ ubiquitous position as watchers and reporters of everything, can be a source of pressure.

**The Low Cost of Failure:** It appears to be easier and cheaper to pass security losses on to customers and to hire lawyers to write contractual terms that hold their organizations harmless, than it is to develop a greater culture of security among users, producers and testers of software.
Breakout Session Three: Security and Organization Structure

The workshop divided into three groups to discuss the demand in security and organizational structure: how security is infused in non-security jobs; how security is aligned with the organization's business and culture; and how demand is appropriately expressed to human resources. Following the one-hour breakout sessions, the full group reconvened to hear and discuss the findings of each breakout.

How Security is Infused in Non-Security Jobs

An Inadequate Emphasis on the Security Role: In general, security responsibilities are not well integrated into non-security job descriptions. This shortcoming is related to a prevailing lack of understanding of the costs and benefits of doing so. We know that employees who are untrained in security protocols, or who don't take them seriously, create risk. However, we don't have the tools to quantify that risk, so it is difficult to make the business case for better security practices.

Different Roles Require Varying Levels of Expertise: Training needs range from the general user (e.g. basic hygiene, password protocols) to management (e.g. security knowledge to inform resource allocation) and cyber support staff (the “front line”—often the first people to recognize something is amiss in the systems they manage). Security responsibilities also vary for non-security employees in different industries. Finance, healthcare, and technology require different security protocols. In all of these fields, inattention to security is potentially damaging to the enterprise.

The Public Health Parallel: The IT environment is comparable to public health in many respects. In both cases, a variety of specialists work together to defend against a range of dynamic threats, but the most effective form of prevention is simple hygiene. Wash your hands to prevent flu. Don’t open unknown attachments to prevent cyber attacks. Infusing good computer hygiene habits at the base-user level is an essential component of cyber security. The health analogy extends to the risk profile as well. Just as infectious diseases spread more rapidly and create more damage in crowded cities, the ever-increasing speed, connectivity and ubiquity of IT multiplies the risk and potential consequences of security failure.

Education Creates Demand: Workers in every IT-dependent industry need to recognize that cyber security failure affects them and their enterprise. Education is therefore a key driver of demand. It is hoped that employees who understand the risk are less likely to grumble about password protocols and other security measures. Informed users, including base-level users, managers, and non-security IT staff, are more likely to take security seriously, to request security training, and to stay current with evolving security protocols.

How Security Aligns with Organizational Business and Culture

Security is Often Seen as an Obstacle: Security in many organizations is seen as something that hobbles action. This “culture of no” can cause resentment and poor
compliance. There is frequently a desire to circumvent security in pursuit of “real work.” As one participant noted, “To the extent that security is seen as something that gets in your way by telling you ‘no,’ people are going to disrespect it.”

**Security as an Enabler:** Security can be seen as a benefit if it enables activities that enhance profitability. If better security practices mitigate the risk inherent in outsourcing, (e.g. allowing a production facility to move safely to a country with significantly lower costs), decision-makers will view security as a net contributor to profitability rather than a cost. In this case, security adds, acting as a very powerful incentive.

**Regulation Changes Culture:** Punitive measures at the highest echelons (e.g. legal liability, or government regulation with real teeth) have a track record for shifting corporate culture toward better security practices. For example, the Sarbanes-Oxley Act had a profound effect on U.S. accounting practices. The Health Insurance Portability and Accountability Act resulted in more rigorous attention to privacy—and by extension to information security—throughout the U.S. health care industry.

**A Near-Failure is a Failure:** Participants noted that it’s difficult for security people to take credit or be rewarded for their actions. Reporting a “near-failure” is not considered evidence that security is working; the near-failure is often seen as a miss. By contrast, in baseball, a relief pitcher who preserves his team’s lead through the last innings of a game is credited with a “save.” There is no similar cyber security reward for helping to avert a failure. Instead, the organization’s reward for good security is continuation of the status quo—the avoidance of negative consequences that become known only in the event of failure.

**Personal Investment:** Good security requires personal investment, but creating investment on an individual level is a real challenge. Personal investment is generated when employees see consequences for their actions: How will my work life be affected by this behavior? Organizational cultures are defined by the behaviors that are rewarded. It is important to develop a culture based on a positive, rewards-based approach to security education and compliance.

**How Demand Is Appropriately Expressed to Human Resources**

**Dual Function:** The human resources department in an organization has two functions: human resource development and human resource management. Human resource management is tactical and short term. Human resource development is far-looking and strategic.

**Framing the Need:** Human resources management personnel are seldom versed in cyber security. Without fluency, they may not succeed in recruiting the necessary skills, even when they are equipped with a good job description. At the National Security Agency, human resources personnel spend time working with cyber teams so they may develop a better understanding of the capabilities those teams require. For human resources to
understand recruitment needs, they need to know the qualities and skills they are looking for in new employees.

**Skill Sets, Not Capacity:** Human resources management tends to think in terms of capacity (e.g. meeting a certain staffing level). The focus should instead be on the skill sets required, and in what combinations. One participant described development of a survey instrument to evaluate competencies on a day-to-day basis. Overlaps and correlations in responses allow creation of discrete skills categories, which can then be communicated to educational institutions to help them develop appropriate curricula.

**The Power of Terminology:** Referring to non-technical analytical and communication skills as “soft” devalues their importance. However, these skills are critical to many cyber security roles. It’s not enough to have the technical abilities; security people must also communicate their needs to management.

**Forecasting the Need:** One panelist expressed a desire for a national report card of the health of the cyber security workforce to articulate a strategy for national workforce development. Such reporting can be accomplished only by establishing a current baseline, setting standards, and then performing a gap analysis. Analysis tools should be developed to forge understanding not just of tasks but also of necessary skills to explain future cyber worker needs. It is difficult to identify specific needs without such a tool, but NSA’s best practice model could be leveraged throughout government and business.
Key Insights and Recommendations

During the workshop’s final session, Shari Lawrence Pfleeger, the I3P’s research director, led a discussion about what participants had learned in the workshop, and what the next steps should be toward understanding demand. Among the primary themes were the need for better measurement tools; more effective communication of security needs to decision-makers; and development of a flexible taxonomy of cyber security skills and responsibilities.

Key findings:

Close the Articulation Gap: Although many workshop participants pointed to a data gap, there is a larger issue: an articulation gap. Incompletely-articulated knowledge, skills and abilities categories and data are available with which to codify and quantify the need for cyber security workforce development. But we also need to articulate value and measure security. That is, we must be able to express the problem and demand in ways that are understood by an organization’s managers within the organization’s culture. For example, if other managers are asking for resources in the context of increasing market share, then security has to be framed as a market share issue, too. Likewise, if the needs are framed financially or in terms of employee retention, then security has to be framed that way, too.

Without careful, consistent ways to articulate the need, institutional knowledge about the role of cyber security in an organization cannot be effectively conveyed to the organization’s decision makers. In other words, security managers know what their specific needs are, but lack sufficient or appropriate tools to effectively advocate for resources. Closing this gap should be a high priority. As one participant said, “You have to show that security has an impact on the bottom line.”

Communicate the Demand: There is a difference between demand for security and need for security. Every organization has security needs, but not all organizations demand security or devote sufficient resources to it. Security in most organizations is not considered a mission function. The need becomes apparent only when security has broken down, or when it is communicated in terms that management can understand. The challenge is therefore to better communicate those needs to decision-makers.

Doing so effectively requires better data and analysis. It requires an understanding of current trends, and the ability to extrapolate demand from them. It requires speaking language that managers, lawmakers and executives understand. Making the investment case is important. Decision-makers should understand that relatively modest investments in cyber security could save multiples later. A challenge is how to raise the alarm without being alarmist.

Define the Range of Security Responsibilities: Effective cyber security requires the active participation of a wide range of people, including system users, managers, IT support staff, generalist IT security professionals, and specialist IT security professionals. Only the latter two will have security as the core focus of their training and experience, but much of the cyber security battle will be fought by rank-and-file IT staff. Likewise, management controls
resources and organizational culture, while base-level users represent the most likely entry points. Therefore security and IT hygiene must be part of the training and job description at every level. One participant noted that while security may nominally account for 20 percent of an IT staffer’s job description, it could account for 80 percent of that person’s potential impact on the organization. In the event of a breach, that 80 percent impact could be negative.

Hire or Train? Yes: Should organizations hire IT security professionals trained in universities, the military and professional schools? Or are they better off hiring people with basic skills and training them within the organization—and the specific systems—they want those professionals to defend? Most workshop participants agreed that the answer is not one or the other; it is a blend of professional training and on-the-job experience.

Compliance is a Double-Edged Sword: Government regulation has been a significant driver of demand for cyber security professionals in some industries. For example, in healthcare, a field that in many ways is analogous to cyber security, HIPAA created an instant spike in demand for certain professionals. Likewise, the Occupational Safety and Health Administration (OSHA) created an entire industry built around compliance. Regulation has the effect of focusing management attention on compliance. It generally creates an increase in demand and in the level of resources dedicated to filling that demand. However, this increased effort is directed at achieving compliance, rather than demonstrated increased security. Training a workforce to fill a compliance requirement is very different from training a workforce to meet an evolving real-world security need. In heavily regulated industries, focus should be placed on aligning compliance with the cyber-security needs of the organization.

Build It as We Go: It is essential to develop credible tools to better measure demand, but we can’t wait before taking action. The demand for trained cyber security operators is evolving and expanding as rapidly as technology itself. It therefore is imperative to build training capacity at the same time we develop the methods to more accurately forecast future needs.

Demand is Unknown, but Growing: Computers and related technologies are becoming increasingly ubiquitous, and as we move into the future our reliance on them will only grow. This dependence is sustainable only if it is accompanied by adequate cyber security. In other words, cyber security is a fundamental, enabling aspect of economic growth and technological advancement. If we want to continue to reap the rewards of greater technological dependence, we must pay attention to security. As one workshop participant noted: “Over this whole two-day period, there hasn’t been one discussion that in any way bent the demand curve down or even slowed it. The demand curve is going up no matter how you describe it.”

Preparing for the Unknown: The pace of technological advance consistently outstrips training curricula. Cloud computing, the proliferation of smart phones, the rise of social networking, the increasing reliance on cellular networks for banking services in the
developing world—all these developments have changed and challenged the cyber security landscape. While cyber security's core mission and its underpinning skills remain largely the same, cyber security professionals must adapt to technological change to remain effective. As one participant noted, “Every job I’ve had in the last 20 years didn’t exist 20 years ago.” Because this technological evolution will continue for the foreseeable future, cyber security training must be grounded in the basic elements of attack, threat, vulnerability and control but remain flexible in the way those elements are interpreted, taught, and applied.