Comments on Cyber Workforce Issues

Robert F. Brammer
Vice President and Chief Technology Officer
Northrop Grumman Information Systems Sector

Panel on Industrial Cybersecurity
CyberFutures Conference – Air Force Association
Washington DC
31 March 2011
Comments on Cyber Workforce Issues

Robert F. Brammer
Vice President and Chief Technology Officer
Northrop Grumman Information Systems Sector

Introduction

This panel today is addressing the issue of how to obtain the right people for the broad array of highly technical, managerial, and policy roles related to cybersecurity. As President Obama has said, this workforce must be strong to keep America competitive in a cyber-dominant world. This significant national problem is the subject of some recent national-level reports and many corporate business plans.

For this panel discussion, I will address two questions about aspects of the cybersecurity workforce challenge from the perspective of Northrop Grumman. The cybersecurity workforce challenge that we face as one of the largest providers of security systems and services to the US public sector is representative of the challenges faced by many large corporations in our industry.

- What are the major challenges in identifying, recruiting, and retaining the right talent?
- Do current industry career paths make sense?

What are the major challenges in identifying, recruiting, and retaining the right talent?

To address this issue, we must provide the context for “right talent” and answer the question “Right talent for what job in what environment?” At Northrop Grumman, we describe our cybersecurity skill needs at three levels.

First, all of our employees need to have basic skills in cybersecurity. Without a broad fundamental skill base and awareness, even the best security systems fail. Materially increased digital literacy for all end-users could lead to significant improvements in cybersecurity. Applying well-known and available solutions could prevent the large majority of cybersecurity incidents. Many of these solutions involve practices with which all employees should be familiar. Our employees must know how to use our access management system, how to protect their identities, how to recognize malware and penetration attempts like phishing, and other such threats.

Second, our systems architects, design engineers, software developers, and other professionals delivering our information and engineering systems and services to our customers need to know how to
embed strong security in from the beginning. Cybersecurity issues are not only about computer science, more network geeks, PC’s, and enterprise networks, but also about systems and services for national security, energy, healthcare, transportation, finance, and many other areas critical to our country and to our customers. Without knowledge of secure design and development principles and recognition of the priority of security, systems will continue to have needless vulnerabilities.

Finally, we need specialists who provide cybersecurity systems and services to our customers and our own operations and researchers who will develop the next generation of cybersecurity policies, processes, and technology. In summary, we will not solve the problems related to the “Human Capital Crisis in Cybersecurity” without a broad view of the issues. Training more network geeks is not the only need. We must address the full range of issues including not only technology, but also economics, psychology, law, and government policies.

Much of identifying the right people for cybersecurity is no different from identifying the right people for any position. We look for intelligence, energy level, attitudes, skills, and experience. However, as many recent reports have shown, there is a critical shortage of skilled cybersecurity professionals. Accordingly, specifically for cybersecurity, we have made many investments that are critical to identifying, recruiting, and retaining this talent. These investments contribute materially to a corporate culture that values cybersecurity as a high business priority. We have invested in the education and training of our staff. We have a tuition reimbursement program, and some of our staff members have completed advanced degrees in cybersecurity. We have developed our own Cyber Academy with a number of courses for all levels in the organization. Our Cyber Academy courses include those for corporate executives, network administrators, software engineers, and military cyber warriors. These courses complement those available from universities and professional certification programs. We have designed courses for our employees at all organizational levels, including senior executives, cybersecurity specialists, and entry-level positions. We plan to enroll more than 1000 of our employees in these courses this year.

We have also invested in advanced research projects and state of the art cyber laboratories, focused on key aspects of pushing the state of the art in cybersecurity. We have developed a research agenda that is a key part of our cybersecurity business strategy. Part of our approach to addressing this research agenda is to develop a strategy for the research workforce. To aid in this development, we have established joint research programs with the world’s leading cybersecurity research universities. These include notably Carnegie Mellon, MIT, and Purdue in our Northrop Grumman Cybersecurity Research Consortium.

---

4 Brammer, Robert, “Panel on Emerging Cybersecurity Technologies,” USSTRATCOM Cyberspace Symposium, Omaha, Nebraska, May 26-27, 2010
We have extended our cybersecurity workforce development investments to the college and high school levels in order to help to build an expanded future generation of cyberspace experts. Among our many sponsorship efforts, we are the Presenting (i.e., major) Sponsor of the Air Force Association’s CyberPatriot competition whose finals are a part of this conference. Dozens of our employees have mentored teams in this competition, and some of those teams are here in the finals. We hired some of last year’s winners into intern positions, and we expect to hire some of these current competitors. We will help others in their college educations by providing scholarship funds to the CyberPatriot program.

These investments have helped to build our growing cybersecurity business. This business base provides excellent career opportunities and the staff depth that enables us to attract and evaluate job candidates. As a result, we have the resources to continue to develop and retain them for their careers at Northrop Grumman. This staff depth is critical in identifying and recruiting candidates. Since there is a lack of standardized qualifications for cybersecurity professionals, it is often difficult for relatively inexperienced management teams to evaluate candidates. We use our large business base and the above investments both to attract candidates and to evaluate their abilities for success in our environment.

**Do Current Industry Cybersecurity Career Paths Make Sense?**

Many organizations are beginning to address the issue of career paths for cybersecurity professionals. This includes some important initiatives in the federal government. Currently, many federal agencies are addressing their cybersecurity needs through contracting, but they also have requirements for some in-house capabilities. Accordingly, the Office of Personnel Management has undertaken a significant effort to define competency levels for cybersecurity, which are helpful in addressing some career path issues.

At Northrop Grumman, we work extensively on the issue of technical career paths. This is essential to attracting highly capable people to join our cyber workforce and to address their continuing professional development.

We have promoted some of our cybersecurity professionals into management positions, both within cybersecurity units and to more broadly based positions. Some of these positions are at the Director and VP levels. We have selected a few as Northrop Grumman Information Systems Technical Fellows for truly exceptional technical contributions. In time, the breadth of issues addressed in cybersecurity will provide a strong background for senior technical management positions across all aspects of our information systems business. We have not yet had a cybersecurity professional become

---

7 [www.uscyberpatriot.org](http://www.uscyberpatriot.org)
8 CSIS Commission on Cybersecurity for the 44th President, “A Human Capital Crisis in Cybersecurity,” Center for Strategic and International Studies, July 2010, pp. 5-9
a sector president or corporate CEO. However, I believe that could happen someday because of the growing importance of this field within our corporation and business base. While we certainly do not have all of the answers, I have seen significant progress in the past couple of years in showing the potential for developing cybersecurity careers.

**Concluding Remarks**

In conclusion, expanding the cybersecurity workforce is a critical issue for the United States and a critical business issue for Northrop Grumman. Doing this requires investments in education, training, and research. We also need good processes for recognizing the contributions of cybersecurity professionals and for rewarding them in their career developments. I know that we are making progress, but I also know that there is more to be done. I think that the results of this conference can make an important contribution to addressing this challenge.