A NEED-BASED ASSESSMENT FOR BUILDING A NATIONAL CYBER SECURITY WORKFORCE

Prof. S. E. Goodman
Georgia Institute of Technology
Atlanta, Georgia USA

Presented at
ICETE 2014
11th International Joint Conference on E-Business and Telecommunications
Vienna, Austria
28-30 August 2014

A world of dependency and risk

- In North America and Europe literally millions of organizations have become so dependent on cyberspace that their vital interests are now vulnerable to attack, accidents and design failures that may compromise those interests.
- Most of these millions of organizations are businesses, but there are many others at multiple government levels, NGOs, and academic institutions.
- All of the organizations come to ground in one or more nations.

A world of dependency and risk (2)

- Many experts believe that on balance the situation is getting worse, that new vulnerabilities are being pumped into cyberspace, and that the bad guys are coming up with more sophisticated, scalable, and precise attacks faster that the good guys are coming up with improved defenses.
- In particular, major new developments are introduced without much effective consideration for security, and security tends to come as an afterthought. Examples: the ARPANET, new platforms (desktops, laptops, mobile devices), the cloud, apps, the internet of things.
- And we continue to suffer from the consequences of accidents and design failures in new and old systems.

A world of dependency and risk (3)

- Much good work is being done to try to improve matters.
- But for all that, the technical R&D pipelines do not show much promise for generating solutions that will provide discernable, measureable, readily and massively scalable improvements in cyber security or resiliency for enormous populations of users.
- Nor is there much expectation that a broadly operational engineering science of cybersecurity or software engineering, or a set of voluntary standards and calls for information sharing, or a set of government laws and enforcing institutions, will achieve this end any time soon.
- We have trouble even imagining what a safe and secure cyberspace might look like in any detail (NRC 2007)

Where we stand

- Cyberspace is thus an environment where all dependent organizations are vulnerable and at risk. (Even NSA.)
- But not all are equally vulnerable.
- There are a multitude of products, procedures, standards, and policies that, if appropriately used, can make some users safer and more secure than others. But is takes knowledgeable people to bring these possibilities to bead, and to sustain and update their use.
- An increasing number of organizations are beginning to appreciate this. But not nearly as many that should.

Where we stand (2)

- Our basic premise is that the primary bearer of risk when things go wrong in cyberspace is the organization that has become so dependent on computer-communications systems.
- There is a vast spectrum of these organizations and they have many different forms of dependencies and risk tolerances.
- Their suppliers, customers, and the users of their products and services make up extended networks of further dependencies and risk.

Need, Supply, Demand (NRC 2013)

- ***Need*** is the number and skill mix of cybersecurity workers that are required to provide satisfactory cybersecurity (a judgment that will vary according to who makes the assessment).
- ***Demand*** is expressed by the desired capabilities stated in job descriptions, the number of such positions that are created and available, and the salaries offered to those who have those capabilities.
- ***Supply*** is the number of available qualified workers willing to fill positions.

Need

- As to need, our assessment would argue that every organization that is seriously dependent on cyberspace must have someone (often more than one person) at a respectable level within the organization, and who understands the vital interests of the organization, to be seriously involved with policies, plans, procedures, recovery, reconfiguration, business continuity, etc.
- Even if the organization decides to outsource its cyber security functions to those parts of the information technology industry that provide relevant products and services, there still needs to be be someone within each organization with the responsibility for selecting those products and services to best meet the dynamically changing needs.
- So, if you subscribe to the basic premises of this talk, even crude first order estimates come up with the need for 7 digits worth of people.

Demand

- So how many positions are designated and funded?
- At least 6 digits worth in just the US government and cyber security industry.
- But that falls far short of the millions of organizations in Europe and North America that have substantial dependencies. How many of these other organizations in the private and public sectors have such a person? We do not know.
- Many organizations may not think they need or have such a person. But we would argue that someone must be at least implicitly responsible for that thought or decision, and by default that person has the organization’s information security authority.

Supply

- Who produces millions of people who have or should have those jobs?
- Estimates based on the almost 200 US CAE colleges and universities are easily bounded by 4 digits/year.
- Some unknown fractions of the rest are people from a variety of backgrounds who enter the workforce by moving laterally internally within an organization, from reformed hackers, or people hired after they are out of school with degrees, diplomas, certificates or other credentials from non-CAE sources.

Supply (2)

- Most of the “professionals” in the cyber security workforce as is is often perceived are trained in computer science departments, or in technical schools, or in certificate programs and the like not part of the formal tertiary, degree granting, educational system.
- Few of these people run the organizations that employ them or are close to the primary missions of these organizations.
- Who are the people who run most of the organizations, and how and where are they trained or educated? And how much exposure do they get to the concerns about the risks organizations acquire when they become very dependent on information systems?

Gap Conjectures

- There is a very large need, and that both demand and supply fall far short. Possibly by an order of magnitude.
- Perceived need (including that version presented here) may or may not be close to real need. Definitions and estimates probably vary considerably. But it would be a mistake to make a market argument that organizations know what is best for themselves and real need finds some sort of equilibrium with actual demand (filled and open jobs).
- It is not clear whether the greater gap against need is with demand or supply. The answers will be dependent on definitions.

Some thoughts to take away

- The primary point I am trying to make is that each cyber dependent organization is largely responsible for its own information security and that it must explicitly recognize this, and have someone in the organization who is explicitly responsible.
- Each organization needs to have someone who is in a position to map available cyber security resources against the vital interests of the organization, and decide on what risks to accept. The supply system is not producing a lot of people who can effectively do this.
- This is likely to leave us with a 7 digit shortfall.

Some Precedents

- We might note that over the last two decades at least two clusters of technological innovation have each resulted in the creation of IT-workforces numbering in the millions.
- One centers on the Worldwide web.
- The other on cellular telephony and other mobile devices.
- But most of the rapid growth in the workforces for these two domains is market or functionally driven.
- Cyber security is different. It has never been market driven to anywhere near the extent as the other two areas. By no means does every organization with serious cyber dependencies see the necessity of suitable cyber security in the ways they see need for a Web site or mobile devices.
- Therein lies a large part of the large scale cyber security need-demand-supply challenge.

Selected References

- NRC 2007, ***Toward a Safer and More Secure Cyberspace***, National Research Council, Computer Science and Telecommunications Board, The National Academies Press, 2007.
- NRC 2013***, Professionalizing the Nation’s Cybersecurity workforce? Criteria for Decision Making***, National Research Council, Computer Science and Telecommunications Board, The National Academies Press, 2013.
- NRC 2014, ***At the Nexus of Cybersecurity and Public Policy***, National Research Council, Computer Science and Telecommunications Board, The National Academies Press, 2014.
- S. E. Goodman, “Building the Nation’s Cyber Security Workforce: Contributions from the CAE Colleges and Universities,” ***ACM Transactions on Management Information Systems***, Vol. 5, No. 2, Article 6, 9 pages, July 2014.