Analysis of Cloud vs. Local Storage: Capabilities, Opportunities, Challenges

Leviathan Security Group

leviathan
security group

limitless innovation. no compromise.

The Scarcity Problem

Employee scarcity is the term that describes employers being unable to recruit sufficient talent in a given niche to fill their requirements. Employee scarcity is generally said to occur if, adjusting for lower-than-market wages and other recruiting path issues, positions remain unfilled for more than one month.[12] This measure of scarcity has been repeatedly validated through peer-reviewed study since the 1960s.

In the cybersecurity arena, there is a general sense that hiring is difficult, and the numbers back that conclusion up. With more than one million cybersecurity positions unfilled worldwide,[3] currently-identified security needs couldn't be met if every employee at GM,[4] Costco,[5] Home Depot,[6] Delta,[7] and Procter & Gamble[8] became security experts tomorrow. Those one million positions span industries, specializations, and requirements; in addition, approximately 25,000 of them are in the United States' federal civil service.[9] These non-military government agencies, in addition to the general difficulty of hiring security personnel at this time, have the added complicating factor of not being able to raise their salaries in response to market conditions. While some authors tout the idea that working for the government brings side benefits that private industry cannot match (such as a sense of giving back to the community and country), these benefits are apparently insufficient to meet the current demand. The military is also interested in locating additional cybersecurity experts, but their approach is to produce them internally (through rating schools and other educational methods), rather than sourcing them externally, so their numbers and internal recruiting concerns are not included in this analysis.

To be clear, this is a global problem which affects every country, regardless of apparent level of technological integration. Few countries' governments can match private salaries, and even private industry is unable to hire sufficient security expertise to meet the demand.

With more than one million cybersecurity positions unfilled worldwide, currently-identified security needs couldn't be met if every employee at GM, Costco, Home Depot, Delta, and Procter & Gamble became security experts tomorrow.

Import or Educate

There are essentially two categories of solutions at the nation-state level for solving long-term significant shortages in specialized employees; a state can choose either to import such talent, or to create it internally. These solutions are not mutually exclusive, but they each have limitations.

The first category of solutions to a country that has a shortage in qualified security workers involve finding expert security workers in other countries, and bringing them (on either a temporary, as-needed, basis, or on a permanent one) to the country with the shortage. In some regions, this can be implemented effectively through existing arrangements. For instance, in the Schengen Zone (the European Union, minus the United Kingdom and Ireland), unrestricted visa-free immigration for any purpose allows workers to respond with very little friction to any employee shortage within the region. There are no strongly-verified numbers on Schengen migration due to needs in the security industry (not least because, in a visa-free union, only post-hoc sampling could find such numbers), but it seems likely that wealthier nations within the Zone are able to offer higher wages to attract cybersecurity experts from poorer nations.

The United States, being significantly more massive than the other partners in the NAFTA low-friction visa zone, cannot take as many security experts (as a percentage of the total needed) from the NAFTA zone. In addition, as the list of permitted professions was assembled during the original negotiations, NAFTA does not contemplate cybersecurity experts independently of related professions such as computer systems analyst, engineer or management consultant. This further complicates a strong understanding of the actual number of professionals working in cybersecurity under a Trade NAFTA Status.

To import talent from outside the NAFTA region, the United States has created another means of importing security expertise: issuing special visas to experts. The H1-B "Specialty Occupation" visa is a program created by the United States to import technical experts from elsewhere into the country for private industry.[10][11] (The US civil service

cannot recruit from the H1-B pool.) H1-B visas require significant technical expertise; at the current H1-B cap levels, 20,000 people holding a Master's degree or higher are chosen to participate in the program, followed by a further 65,000 people holding at least a Bachelor's degree (though these people, too, often hold additional degrees). In order to obtain permission to hire someone under an H1-B visa, companies have to assert that they are unable to hire the needed expertise within the United States.[12] The vast majority of H1-B visas—68%—are for computer-related jobs, of which the majority of positions are, in turn, related to security.

Three major American firms—SAIC,[13] Booz Allen Hamilton,[14] and 3M[15]—list a combined 2,986 unfilled positions on their H1-B-specific cybersecurity recruiting pages as of July 28, 2014. The 2014 H1-B visa cap was filled to more than twice its quota (for a lottery) on April 7, 2014, six days after it opened.[16] Presumably, these positions will stay unfilled at least until October 2015, when the application window will open again. Visa renewals are not included in the cap, so experts who come to the United States under the H1-B program can (and, presumably, will) stay indefinitely without ever returning to their countries of origin.

Just three U.S. firms list nearly 3,000 cybersecurity positions they cannot fill with Americans; those experts that eventually fill the positions may never return to their home countries to provide expertise there.

These 85,000 experts—representing approximately 57,800 computer experts, of whom a significant percentage are security-related—do not magically appear on a global scale, however. Necessarily, each security (or other) expert drawn from another country, while representing a gain to the knowledge pool of the United States, represents a loss of experience and talent from their country of origin. While Article 12 of the International Covenant on Civil and Political Rights requires countries to allow emigration (in most cases), a "brain drain" on this scale may be considered, at the extreme, a threat to the national security of the countries of origin.

The second category of solutions involves training domestic persons to a sufficient level of expertise in security. Most of the Global North and BRICS countries (Brazil, Russia, India, China, and South Africa) have one or more government-supported educational initiatives to identify and train cybersecurity talent, ranging from educational scholarships to intelligence-agency-led curriculum design, that apply to every level from secondary education to PhD programs.[17][18][19]

These programs cannot, however, scale quickly or effectively enough to deal with the outsized nature of the demand for expertise. To take one illustrative example, the entire United Kingdom's advanced, GCHQ-led cybersecurity programs will produce just 66 PhDs with a cybersecurity focus per year—beginning in 2017. The UK has also invested significant resources in including more security work in general engineering and computer science programs (for instance, by requiring at least one course on security in all accredited engineering programs beginning in 2015), but this single additional course—in effect, just another breadth requirement within computer science and engineering, among the many others that exist already—will not be able to educate even the UK out of its talent shortage, let alone the world. The UK (among many other countries) is also attempting to kickstart the education of security practitioners at sub-expert levels, for instance by recruiting 100 students per year to take a two-year "Foundation Degree" program of study designed by GCHQ. While educating students at a basic level will, in time, motivate some of them to proceed on with their education and attain mastery, this is a many-year process with no gains at the expert level in the short and medium term.

Across the broader European Union, the European Commission's TEMPUS (Trans-European Mobility Program for European Studies) program, an educational development initiative that seeks to create educational initiatives across the EU, Eastern Europe, the Near East, and North Africa, cataloged the curricula, requirements, and desired outcomes of cybersecurity education programs, both inside the TEMPUS regions and around the world. It documented new Bachelor-level security programs in the UK, Russia, China, the US (using the University of Maryland at University College's program as an exemplar for NSA-led curricular change in a semi-professional degree setting), Canada, and Australia, but noted that these have limited utility; "Master degrees are essential for providing a cybersecurity workforce with advanced capabilities."

A GREAT DEAL OF TIME, MONEY, AND ATTENTION IS BEING FOCUSED ON CYBERSECURITY WORKFORCE DEVELOPMENT, BUT IT IS STILL UNCLEAR WHAT LONG-TERM EFFECTS THAT WILL HAVE ON THE SUPPLY OF CYBERSECURITY PRACTITIONERS, ESPECIALLY AT THE EXPERT LEVEL.

TEMPUS found much smaller Master-level programs in Estonia (another consequence of Estonia's 2007 digital attack, in addition to the establishment of the NATO Cooperative Cyber Defence Centre of Excellence being established there, the "Tallinn Manual on the International Law Applicable to Cyber Warfare" being authored there, and the annual NATO CCD COE conference on cyberwarfare being held there), the United States (this time using the University of Maryland at Baltimore

County's Professional Studies program as the NSA-led exemplar), Australia, and the United Kingdom. Finally, it found doctoral programs in the United Kingdom, the United States, Germany, France, Estonia, and Norway. However,

> *While doing research for these examples, [TEMPUS] found that while cyber security is well represented among master study programs, the number of Ph.D. programs specifically targeting cyber security is not very high. The majority of Ph.Ds. in the cyber security field are researched and awarded during studies of a more generic kind, ordinarily computer science, without a devoted Ph.D. program.*

In addition to educational programs, business and non-profit groups are trying to stimulate interest both in STEM fields generally, and on cybersecurity specifically through sponsoring events, diversity pushes, and funding grants to schools and other entities. A great deal of time, money, and attention is being focused on cybersecurity workforce development, but it is still unclear what long-term effects they will have on the supply of cybersecurity practitioners, especially at the expert level.

Conclusion

While this report has focused on the educational programs being launched and/or upgraded to train additional cybersecurity talent, it is important to realize that education is not the same thing as expertise. Even very-well-trained students from commendable degree programs will require time and experience to reach the level of expertise required of them. Beyond a certain point, putting more money into the problem will prove ineffective to shorten the time it takes to develop new security expertise.

This analysis has focused primarily on talent shortages in the Global North, especially on Western Europe and the US; this is both because insufficient data exists on other regions, and because the technology infrastructure is less advanced in most other regions. As Africa, the remainder of South America, and the remaining Asian countries build out their infrastructure (as they are doing at an extremely rapid pace), their needs for advanced security practitioners will necessarily increase.

In the future, countries that depend on "locking in" their security talent (whether that talent comes from that country or another) by moving the personnel from one country to another will face competitive "bidding wars" between companies and nations. A more sustainable idea may be to encourage the sharing of talent and technical resources; this would allow the world as a whole to secure fewer pools of critical data, rather than a multitude of balkanized networks. This, in turn, would lower the number of needed security experts—not enough, in the near term, to alleviate the shortages discussed in this paper, but this strategy could avoid worsening the problem.

Taken together, then, these factors indicate that it may not be possible for the vast majority of countries to source the necessary security expertise to secure their infrastructure locally. Since security practice is something that can be done across national boundaries, it seems increasingly clear that a significant amount of security expertise must be shared, at least in the short and medium terms. Any plan that requires a country to source locally its security talent, its data, or its computational infrastructure may be requiring the impossible—and harming the country's ability to secure its industry.

Even very-well-trained students from commendable degree programs will require time and experience to reach the level of expertise required of them.

Notes

1. "Employment Service Operating Data as a Measure of Job Vacancies," Chavrid and Kuptzin, in "The Measurement and Interpretation of Job Vacancies," National Bureau of Economic Research (1966)
2. "H-1B Visas and the STEM Shortage: A Research Brief," Rothwell and Ruiz, Brookings Institution (2013)
3. "Cisco 2014 Annual Security Report," https://www.cisco.com/web/offers/lp/2014-annual-security-report/index.html
4. "GM 2013 10-K Filing," http://www.sec.gov/Archives/edgar/data/1467858/000146785814000043/gm201310k.htm
5. "Costco 2013 10-K Filing,"http://www.sec.gov/Archives/edgar/data/909832/000119312512428890/d388097d10k.htm
6. "Home Depot 2013 Five- Year Summary," http://www.homedepotar.com/pdfs/home-depot-2013-five-year-summary.pdf
7. "Delta 2013 10-K Filing," https://www.sec.gov/Archives/edgar/data/27904/000002790414000003/dal1231201310k.htm
8. "Procter & Gamble 2013 10-K Filing," http://www.sec.gov/Archives/edgar/data/80424/000008042413000063/fy201310kannualreport.htm
9. http://www.sdbor.edu/theboard/agenda/2014/April/26_1a.pdf
10. "H-1B Fiscal Year (FY) 2015 Cap Season," http://www.uscis.gov/node/41921
11. There are other types of H-1B visas, including the H-1B2 visa, reserved for multi-governmental research backed by the Department of Defense, and the H-1B3 visa, reserved for fashion models of international prominence; neither of those will be included in this discussion.
12. "H-1B Visas and the STEM Shortage: A Research Brief," Rothwell and Ruiz, Brookings Institution (2013)
13. https://jobs.saic.com/key/cyber-security-jobs-h1b.html
14. http://careers.boozallen.com/key/cyber-security-jobs-h1b.html
15. http://jobs.3m.com/key/Cyber-security-H1B-jobs.html
16. "USCIS Reaches FY 2015 H-1B Cap,"http://www.uscis.gov/news/uscis-reaches-fy-2015-h-1b-cap
17. "The National Cyber Security Strategy Our Forward Plans - December 2013," Office of the Cabinet, United Kingdom (2013)
18. "Hackers Wanted," Libicki, Senti, and Pollak, RAND Corporation (2014)
19. "Report on EU practice for cyber security education," European Commission TEMPUS (2013)

Project Team

- **James Arlen** - Director of Risk and Advisory Services - james.arlen@leviathansecurity.com
- **Lee Brotherston** - Security Advisor - lee.brotherston@leviathansecurity.com
- **Steve Manzuik** - Security Advisor - steve.manzuik@leviathansecurity.com
- **Brendan O'Connor** - Senior Security Consultant - brendan@leviathansecurity.com
- **Chad Thunberg** - Chief Operating Officer - chad.thunberg@leviathansecurity.com

Leviathan Security Group, Inc.
3220 1st Ave S, Suite 100
Seattle, WA 98134

p: 866.452.6997
f: 206.225.2004
e: contact@leviathansecurity.com

www.leviathansecurity.com

This work was commissioned by Google Inc., and created by Leviathan Security Group, Inc.
Google had no editorial control over this document.