



The Datagram

newsletter

July, 2017

Volume 2, No. 7

From the Chair...

How's your job? Do you have job, career, and salary security? Looks good now, but what about ten years from now? Or twenty? It's hard to get a job when you're 40. Harder yet when you're older. So how about it? Will you have a job?

Nice questions. Your career in cyber security is probably certain. Any new innovation to restrict or eliminate hackers (spam, ransomware...) seems to be effectively met by them. And the lines of code/applications are so large that the probability of having some hidden pathway to cause damage is almost certain. This translates to a current and ongoing need for Cyber Security personnel. Your career seems to be secure.

Adam Smith's "Hidden hand" and modern economic theory dictates that where there is a demand, then a product can be "sold." As the demand grows or the 'product' quantity is insufficient to meet the demand, the price grows. So, you are currently in demand and currently there aren't enough of you. Now!

Continued on page 2

Next meeting:

July 26, 2017

6:30 PM Dinner and Networking
7:00 - 8:00 PM Presentation
8:00 - 8:30 PM Q & A
8:30 - 9:00 PM Meet & Mingle

Dinner: FREE

ATEP, 15445 Lansdowne Road,
Tustin, CA, Room #D106
(Room number subject to change)

Speaker: Gora Datta

This Month's Topic: How Cyber Security is Redefining the 21st Century IoT World of Digital Health

With the phenomenal rise of mobile devices globally in the past decade, we have now entered the digital age. We have gone through the agricultural age, the scientific age, the industrial age, the information age, and now we're in the digital age! This global transformation is bringing a change that is impacting our world in every way - how we interact, play, read, write, watch, study, research, work or even relax. Soon we will live in a world that is interconnected with Internet of Things (IoT).

Continued on page 2

A b o u t t h e

Speaker

Gora Datta, HL7 International Ambassador, is a US-based ICT Subject Matter Expert. He is an accomplished, visionary executive with 33 years of international professional expertise in the field of computer and software engineering and its application to health-care, mobile health, cybersecurity in healthcare, eLearning and social protection. His global professional experience spans many countries: Australia, Bangladesh, Canada, France, Greece, India, Indonesia, Japan, Kuwait, New Zealand, Niger, Norway, Philippines, Singapore, South Korea, Spain, Switzerland, Tunisia, UK, and USA.

As a global healthcare IT standards expert, Gora is actively involved with various standards and professional organizations:

- Health Level Seven (HL7) International (2002 - current)
- (founding) Co-Chair HL7 Mobile Health Work Group (2012 - current)
- ISO TC215 Health Informatics: USA Country Delegate (2008 - current)



From the Chair, *Cont'd.*

Look about you. Each school at the community college, college, and university level has a school in Cyber Security. Each private school has a course, and there are multiple online (free and not-free) courses. The supply of the "product" is increasing. Never mind the skill level. Institutional hiring is often based on price—to the exclusion of skill.

This means that your salary is in jeopardy. With more graduates with certifications and/or degrees in cyber security, there is more competition at the supply end. We are faced with a limited demand and an expansive supply. You, my friend, are the supply.

This means that at a certain point, your current salary cannot be supported because the average salary of new hires will drop. This drop will gradually filter up the food chain to you. When that point is reached, your employer has three options; (1) No raises, (2) reduction in salary or reassignment, or (3) Bye. The "Hidden Hand."

There is no good answer to what to do about this—maybe playing the lotto. There are only a limited number of ways to your improve current skill set and branch out to new areas. And, of course, save to purchase an umbrella when it rains. The standard answers do not apply to everyone. Start a company. Go into management. Change jobs. And so on.

At the end of this rather dismal

forecast, let's look a minute at me, the chief prognosticator. How good am I? Well...I once said that microcomputers would not amount to much.

Art

(reluctant) Chair,
CyberSecurity SIG

July Topic, *Cont'd.*

Healthcare access and delivery is going through a seismic change...rapidly moving from paper to digital health. Health information technology (Health IT) is making it possible for health care providers to better manage patient care through secure use and sharing of health information. However, recent news headings (of WannaCry ransomware attacks in May, 2017) are amply demonstrating the wake-up call....cybersecurity is redefining this changing world of digital health.

This talk will review the digital health transformation that we are undergoing, the challenges of cyber-health that face us, and the mitigation that is critical in the 21st century world (of Blockchain, AR/VR, Precision Medicine, Predictive Analytics, Machine Learning, Cloud Computing and IoT in Health).■

Contact Information

Website: sites.ieee.org/ocs-cssig

[Meetup.com/CyberSecuritySIG](https://www.meetup.com/CyberSecuritySIG)

Newsletter Editor:
stargazer@stargazerpub.com

Is Your Company Cyber-Immunized?

On June 13, 2017, Michael Chertoff, former U.S Secretary of Homeland Security, gave a presentation on the importance of cyber security at the Cyber-tech Fairfax Conference in Fairfax, Virginia. Stressing the necessity for proper risk management, Chertoff advised focusing on company policies and procedures and educating employees thoroughly so that they understand their role. Risk management also includes mitigating human error, he emphasized, an element that is often overlooked. For details, go to <http://inhomelandsecurity.com/chertoff-cyber-immunized/>■

Is Your Company Cyber-Immunized?

According to Dr. Douglas Maughn, Director of the Cyber Security Division of the Department of Homeland Security, industry leaders are constantly on the lookout for innovative technology. He has concerns, however, with tying operational technology (OT) to IT.

Rajeev Barua, founder and CEO of SecondWrite believes that while current cyber security tools detect intrusion, they can't distinguish malware from benign entities. His company has a product currently in beta testing to solve this problem. The expected launch date is in the third quarter of this year. For details, <http://inhomelandsecurity.com/>

Be Aware of Financial Scams

Most computer experts are aware of scams like emails from Nigerian princes asking for your help in depositing money in the U.S. and requesting remote access to your computer to fix it from "problems."

A new scam has entered the arena: a request saying that the local police have a warrant for your arrest. You can avoid jail by wiring money to them.

Another version of this scam informs people that a lawsuit has been filed against them and that they need to call the phone number stated immediately to resolve the issue.

Still another scam is claiming that a person owes money to the IRS. The IRS never asks for money over the Internet or the phone.

James R. Lint, former civilian director for intelligence and security, U. S. Army Communications Electronics Command, urges everyone to report all scams to law enforcement authorities. For complete details on this topic, go to <http://inhomelandsecurity.com/protect-yourself-criminals-financial-scams/> ■

International Cyber Attack

The Associated Press reported that a major cyber attack caused havoc around the world

on Tuesday, July 25th. It is believed to have started in the Ukraine by the Shadow Brokers, a group of hackers who leaked powerful NSA tools.

According to the AP, this attack affected computers at Russia's biggest oil company, Ukrainian firms, India's largest container port, and lab and diagnostic services in Pennsylvania, U.S. drugmaker Merck, food and drinks company Mondelez International, global law firm DLA Piper, and London-based advertising group WPP.

David Hubler stated that "the rapidly spreading computer worm appeared to be a variant of an existing ransomware family known as Petya or ExPetr, which also includes key features from last month's ransomware "WannaCry" attack.

On Wednesday, July 26th, the Shadow Brokers made additional threats, and Kremlin spokesman Dmitry Peskov told a news conference in Moscow that such attacks underline the need for a concerted international effort to fight cyber crime. For complete details, go to <http://inhomelandsecurity.com/cyber-attack-global-ransomware/> ■

Verizon Attack

Most Verizon customers are not aware that a company called NICE has access to their data. A breach exposed millions of customers' data. For details, go to <http://inhomelandsecurity.com/millions-of-verizon-customers-exposed-by-third-party-data-leak/> ■

2017 CyberSecurity SIG

Chair	Arthur Schwarz
Co-Chair	Gora Datta
Treasurer	Brandon Young
Programming	Irvin Lemus
Newsletter	Carol J. Amato
Web Design	Ginson Samuel
Audio-Visual	Open

Place Your Ads in The Datagram

Do you have information about an academic program, seminar, work-shop, symposium, presentation, or job listing related to cybersecurity? Consider placing an ad in The Datagram.

Ads are currently FREE and will be published for three months, after which they are renewable. They will appear simultaneously on the CyberSecuritySIG's website at sites.ieee.org/ocs-cssig for maximum exposure.

Submit a camera-ready, business-card-sized (3.5" x 2") JPG file to Carol Amato at stargazer@stargazerpub.com.

Please Provide Feedback on Our Website

We want your feedback on our new website. If you like what you see or have any changes to suggest, tell us and others. If you have any changes in mind, please let us know. We are open to any suggestions and would appreciate your comments. ■