No Time to Lose: Get Serious About Cybersecurity Education

Mansur Hasib
******@***umuc.edu

Programme Chair of Cybersecurity Technology - The Graduate School of University of Maryland University College (UMUC) & Cybersecurity and Healthcare Speaker & Author

Twitter

Winner of the 2017 Cybersecurity People's Choice Award organised by the Cybersecurity Association of Maryland, Inc., Dr. Mansur Hasib, speaks to HealthManagement.org about how critical effective cybersecurity education is for HIT university students.

What is your advice on how to better equip HIT students with an awareness of cybersecurity in their education?

At several conferences and my classes, I have defined cybersecurity in the following manner:

Cybersecurity is the mission focused and risk optimised governance of information, which maximises confidentiality, integrity, and availability using a balanced mix of people, policy, and technology, which perpetually improves over time.

I have also consistently explained that you cannot and should not overlay cybersecurity on top of anything. All information technology disciplines need to factor in cybersecurity into their education and practice. This is true of HIT, computer science, and computer engineering, as well as any discipline that deals with information creation, storage, processing, distribution, and transmission. Today that happens to be all disciplines.

What are the top three lacks in education when it comes to cybersecurity? Can you give examples of how these lacks have been reflected in the healthcare world?

The education of almost all disciplines is due for a major overhaul and update. Since digital strategy drives the mission of all modern organisations, the educational curriculum of almost all disciplines need to be updated to include digital strategy and cybersecurity principles. The lack of such curriculum in business, healthcare, and other such disciplines has created a serious deficiency in the preparation of students. Graduates prepared through outdated curriculum enter the executive world of healthcare and make seriously flawed decisions, which cause the harm we are seeing at an alarming pace.

How do you suggest educators address these curriculum lacks?

© For personal and private use only. Reproduction must be permitted by the copyright holder. Email to copyright@mindbyte.eu.

Get serious about updating the educational curriculum. All educational tracks must include cybersecurity and digital strategy into the curriculum. Break the cycle of relying on expensive and outdated books being sold to a captive audience of students. Instead provide students with rich flexible and current content, which is usually available at no cost, and update the content regularly.

How do you feel about winning the People's Choice Award in the 2017 Maryland Cybersecurity Awards?

Winning this award was a fascinating experiment and experience for me as well as my students. I teach all my students how to build a personal brand. I teach them that their personal brand must be independent of any organisation they work for, or affiliate with. I explain that a personal brand can be developed through knowledge sharing, public speaking and networking at conferences, teaching, and writing.

I caution people not to affiliate with organisations, which are likely to diminish or tarnish their personal brand. They should assess every opportunity in light of the effect it will have on their personal brand. Most of these activities will also result in alternate sources of income in the event their primary source of income disappears due to circumstance beyond their control.

In an era of layoffs and perpetual job insecurity, where people cannot entrust their career success to a single company, or even the civil service or the government sector, a strong independent personal brand gives individuals better control of their personal and professional success. Technology now allows individuals to amplify their voice and to build personal brands through knowledge sharing and by speaking to others about their passion.

This is critical for their career success and personal risk management. Everyone should strive to achieve a level of personal brand strength so that organisations seek association with their personal brand in order to enhance the company brand. This is the main reason why, despite an inherent danger of diminished authenticity, companies use people with strong personal brands from unrelated fields, such as movie stars, athletes, and even TV anchors, to promote their products.

In this contest, 18 company brands and four individual brands were in contention for global public votes. Since a contest of this nature had never been done before, we all learned an incredible amount. My message has always been about the valuable role people play in cybersecurity and organisational success. I am sincerely grateful to all the people who voted for me, passionately urged others to vote and supported me in this effort. People validated my faith in people.

Dr. Mansur Hasib is a cybersecurity and healthcare leader, author, speaker, and media commentator in the world with 12 years experience as Chief Information Officer, a Doctor of Science in Cybersecurity (IA), and the prestigious CISSP, PMP, and CPHIMS certifications. Dr. Hasib has 30 years experience in leading organisational transformations through digital leadership and cybersecurity strategy in healthcare, biotechnology, education, and energy. Dr. Hasib currently teaches the art of cybersecurity leadership, digital innovation and strategy to graduate students and executives worldwide and is Programme Chair of the graduate Cybersecurity Technology program at UMUC. He is also a cybersecurity faculty at UMBC.

With a Bachelor’s degree in Economics and Politics and a Master’s degree in Political Science, Dr. Hasib has a unique interdisciplinary perspective and can discuss poetry and culture as comfortably as digital strategy, business innovation, and cybersecurity. He is the author of Cybersecurity Leadership: Powering the Modern Organisation (ebook, paperback, and audio), which received two nominations for The Cybersecurity Canon 2016 – the Hall of Fame for cybersecurity books. He conducted a national study of US healthcare cybersecurity and published the book Impact of Security Culture on Security Compliance in Healthcare in the USA.

Published on : Tue, 4 Apr 2017

© For personal and private use only. Reproduction must be permitted by the copyright holder. Email to copyright@mindbyte.eu.