Review:
Certified Cybersecurity Awareness Professional (CCAP) online course

The Internet as we know it today sprung to life in the early 1990s, when roughly 5,000 networks in almost 40 countries served 700,000 host computers and more than four million people. At that time, I was vice president of a software development firm in northern Virginia responsible for a line of encryption products meant primarily for the military, government, and industry. What kept my clients up at night was the possibility the sensitive data and information held within their computer environments ("enterprises") would be stolen. As well, they worried the data could be compromised during its transmission from one point to another. Users of the burgeoning Internet paid little if any attention to security matters except to purchase one of several early anti-virus programs that had been developed.

Today, computer security should be *everyone's* concern! Digital technology, as pointed out repeatedly in this comprehensive cybersecurity course, is everywhere and "touches" everyone almost every moment of their lives. It is estimated there are 5.15 billion unique mobile phone users in the world today. Almost certainly you have a cell phone. How often does it ring without you be told who the caller is? What about those e-mails you get, allegedly from *your* banks and other financial institutions and vendors, asking you to confirm your account information? Did the request look legitimate? Did you click on it? (Shame on you!). What about the baby monitoring system in your infant daughter's room? Did your wife happen to mention your child complaining she had heard voices on it last night? And why did your last phone bill contain an astronomical charge for a call you returned unknowingly to the Caribbean last month when you returned a call you had received when the phone rang only once ("ring and run")?

What I've described above are but a few—a very, *very* few—of the ways in which scammers use the world of digital technology to part you from your data, information, and technology . . . and money! Not to put too fine a point, the results can be devastating, if not fatal, as in cases where the records of entire hospital complexes are held for ransom until management deposits the required number of bit coins in the account of the hackers who hijacked their patients' data.

Think it can't happen to you? Think twice. And protecting yourself begins by educating yourself…educating yourself about the threats you face with each of the devices you use (e.g., cell phone, laptop, VOIP telephone, home security system, etc.) as well as the remedial actions you can take. For example, in the case of the unwitting telephone call to the Caribbean cited above, did you know you can contact your telephone provider and request that no international calls be permitted from any of your telephone numbers? (I learned that from this course, and I took immediate action to implement same.)

This course is a true tour de force when it comes to cybersecurity. Among its attributes is the fact that it is "product agnostic." Unlike many courses you find on this subject that are tied to a product (e.g., an antivirus program or a device intended for cyberprotection), the sponsors of this course are only interested in ensuring you receive a comprehensive education on the issues and threats that impact on you. How and to what extent you implement the suggestions and advice provided is a matter of your

needs, risk tolerance, and ability to withstand the consequences should a threat materialize.

In taking the course, which lasts four (4) hours, I found the material well organized and paced in such a way that the "student" has time to make notes as the speaker and slide presentation moves along. Important points often are **bolded**, suggesting you probably will see material related to them on the certification exam (which, being retired, I did not take). Regardless, the information is multi-level in nature, so whether you are a student or retiree, or employee or security officer, you will find material at a level you can understand and, importantly, put to use immediately in your cyberenvironment. Things as simple (if that's the word) as knowing NOT to answer the phone from callers whose numbers you do not recognize, to opening emails from people you don't know, or from clicking on links or hot buttons within emails ostensibly from "your" bank or financial institution, to sending sensitive information over Internet sites that do not have the "https" protocol sign (signifying encrypted information, though even then you have to be careful), and so forth, are just a few of the many things discussed.

You may think you can spot the thieves, but think again! Here are a sample of the major data breaches in the last 5 years. These occurred at major corporations; they spend tens of millions of dollars every year on computer security. Chances are good (though they won't say) someone in their organizations clicked on a link within an innocuous email, and that was enough to let the thieves enter their domains. Note that even the cybersecurity firm Equifax was "hit." No one—NO ONE—is safe.

The top 6 data breaches in the last 5 years:

- The Yahoo breach: Accounts affected: 3+ billion. ...
- FriendFinder Networks breach. Accounts affected: 412 million. ...
- Marriott-Starwood breach. Accounts affected: 383 million. ...
- Myspace breach. Accounts affected: 360 million. ...
- Under Armour breach. Accounts affected: 150 million. ...
- Equifax.

It also occurred to me as I took the course that much of what I read would be of immense help, say, to a company's corporate security officer. Every firm for which I ever worked in the defense, homeland security, and anti-terrorism sectors had such a person, someone who not only was responsible for security clearances, but also, for employee training. The material found in this course has the potential not only to "seed" such training courses, but also, to add considerably to a course's breadth and depth, especially in the use of corporate email systems, a major vulnerability.

All in all, this course, amazingly, succeeds in providing important material for everyone at every level *without* being mediocre! It is truly a valuable cybersecurity resource that, for the casual computer user, will help to prevent your computer from being compromised, and, for the business, non-profit, and religious user, may, upon implementation of the material presented, one day save you from bankruptcy.

Theodore J. Cohen, PhD
August 23, 2020