Cybersecurity:
Get Ready For Some New Terminology

Rhonda Chicone, School of Business and Information Technology, 2015

Originally published on the “Industry Insights” section of the Kaplan University website.

Cybersecurity: Get Ready For Some New Terminology

Recently I attended a cybersecurity symposium on behalf of Kaplan University. This was the first cybersecurity event I've attended since 2012 and much has changed by way of terminology referring to the cybersecurity domain. Over the course of a day, I listened to talks from members of high-ranking military personnel and private companies like IBM, Booz Allen Hamilton, and General Dynamics.

As I listened to the talks, attended panel discussions and participated in basic networking activities, I heard terms thrown about like “cyber hygiene,” “cyber strong,” and “cyber palette.” Interestingly enough, I contacted a couple of my corporate colleagues, who work as cybersecurity analysts, and they had never heard of these new terms (at least I didn’t feel alone). These terms may just be the latest buzz terms in the cybersecurity domain, but the meaning behind the terminology is important and everyone should know about them.

Cyber hygiene simply means performing basic tasks to protect digital assets. For example:

- Use strong passwords, do not write passwords down for others to see, and change your passwords frequently.
- Validate the sender before clicking on links/URLs within email or within text messages.
- Do not send a Social Security number or bank account number to another person via email.

Again, cyber hygiene is about performing basic, common sense tasks to safeguard what is important in the digital world.

Cyber palette was the most interesting one to me as it reminded me of using Adobe Photoshop and working with palette layers. It is the idea of implementing security in a multilayered way. This is sometimes called “defense in depth.” The basic idea is that any one-security protection mechanism can have flaws, so use additional protection mechanisms in case the flaw(s) are exploited. For example, a company would deploy a firewall to control incoming and outgoing network traffic, but add an intrusion detection or a prevention system to aid in monitoring the network and/or critical systems for malicious activity.

Finally, *cyber strong* means that an organization has taken steps to protect their networks and systems using the cyber palette methodology. This also includes educating personnel about the acceptable use of digital equipment. Cyber strong means that the security posture of an organization is strong and the organization is prepared to defend more sophisticated attacks.

I would be remiss if I didn’t bring up a couple more terms that have been around for a while but that I find relevant more now than ever. Back in 2008, I wrote a chapter for a book that was about cyberwarfare. A cyberwar is just like a regular war, but it is one being fought without using conventional weapons. Instead, the weapons used in cyberwarfare are computers, and the enemy could be 8,000 miles away sitting in their home armed with a computer.

The chapter in the book that I wrote was about mobile devices and how they will become a very popular cyberweapon. The assertions I made in the book were based on my industry experiences and research for my dissertation. Now it is 2015 and as I listened to all the speakers, each and every one of them talked about how mobile devices have disrupted the cybersecurity landscape by introducing yet new challenges for those fighting in a cyberwar.

To me, awareness is the first step in understanding something new. It was important to share some new cybersecurity terminology and their meanings. In my opinion, everyone should know about them, as they are not reserved for those who work in the cybersecurity domain. Be on the lookout for more new terminology in the cybersecurity domain, as it certainly will not stop here.