***IDC 6601 – Final Assignment***

*Setting:  You are still the Chief Information Officer (CIO) for XYZ, Inc.  Having set the proper policies and training in place to correct the situation your predecessor left you with, you now can look at the long-range cyber issues still affecting your cybersecurity workforce's development.*

***(NOTES: for your answers below, use the guidance se­en in the assignments for IDC 6601.  I expect more than a sentence or two for each answer!  Please do proper citations, etc. Single spaced, Times New Roman, 12 font. Use this template and rename the file with your first.last names – you can add spacing to make room for your answers).***

1.  **(5 points total)** Although you fixed the various policy and training issues last Fall, problems remain.  First, you continue to have problems with users in your company going to unauthorized websites and accessing improper content from their work machines.

* What tools/technology can you employ to mitigate this issue? **(3 points)**

**I would take the steps to build a stronger firewall that blocks all unauthorized networks. The company I used to work at (Siemens), for example, implements this really well. I couldn’t access some websites via their network that I could at home.**

**Another step to take is to require employees to sign a contract to abide by all company policies and go thru training on why they should avoid unauthorized websites and the negative consequences of doing so such as company data being compromised and possible termination of employee role.**

* Besides training and technology at the user level, what else can be done? **(2 points)**

**I would have an IT department that occasionally monitors the web browsing behavior of every single employee. For example, my manager at Siemens found out a co-worker was accessing their teams meetings via home network and that was not allowed. It’s amazing that they can still track you using Microsoft teams at home since it goes thru their firewall first before heading to teams.**

2.  **(11 points total)** Now, your IT support folks discover that your systems have been compromised by a phishing attack, which gave the outside attackers admin access to your servers and services temporarily.  The IT support section personnel are still working the issues; but, the good news is that they feel that they have eradicated the threat and are now mostly doing clean up operations.  You institute guidance to your users to assume an environment where you are constantly under attack and institute training to support that guidance.

* Is this type of attack (phishing) predictable considering you thought you fixed the previous problems? Explain your rationale **(2 points)**

**No. I think if it were then the systems wouldn’t have been compromised in the first place. There needs to be action taken to mitigate the issue such as having all the passwords changed in the system, including those of the users. From now on, in fact, users should be required to change their passwords on a periodic basis, much like the way UCF handles students changing theirs.**

* Would an after action report by the IT department be a good idea?  Explain **(2 points)**

**Absolutely. This is a crucial analysis step in the process of the greater improvement in terms providing a secure and safe environment to work in for the company. Two companies I’ve worked at have already implemented such features. Although it may not be always about the cybersecurity aspect, an after action report is a universally applicable tool for assuring the safety and well-being of a company.**

* How realistic is it to require all employees to assume such a mindset where they are under attack constantly? Is that a good idea to do so?  Explain **(4 points)**

**In reality the larger the company, the harder it is to maintain such a mindset. However, with the tools and techniques I’ve previously mentioned, it should make the process easier. This is especially true when machines are helping us do some of the work because machines can avoid human errors.**

* How do we determine the balance between relying on tools (white listing, etc), people (end-user awareness training, workforce development, etc) and procedures (e.g., having active defense processes, etc) to counter attacks?  **(3 points)**

**There comes a time when the company has to know when to over engineer or automate a process. Moderation is key and for now, the cooperation between human and machine is the most ideal in many situations. Too much automation without human monitoring can do more harm than good in many cases. For example, an engineer may automate a webscraper to extract CSV files from a certain website and have that program run on a daily basis. In a situation like that, it is important that there is still periodic monitoring in case, for example, if the url changes slightly, or if certain UI elements change or aren’t where they supposed to be. In other words, no program is perfect, and a human needs to be present from time to time to provide error checking.**

3. **(4 points)** As CIO, you realize that technology has allowed a greater level of anonymity and masking of identities in cyberspace, but have also resulted in the loss of privacy (i.e., can search for others’ personal information on social media, monitor staff activities etc.). Technology has also challenged the definition of ownership and property, and has opened up all sorts of new ways to commit crime in cyberspace.

Drawing on your own work or personal experience, **discuss either (not both)**(i) how technology has profoundly changed the way we live and work (e.g., we behave and conduct various activities differently online), or (ii) how our laws and policies have not kept up with what technology has enabled.

**To answer the first one, I would argue that technology is tool that has provided more benefit than harm. In my opinion, much of the harm side of things can be avoided with proper training and education. The cycle of human factors diagram that was taught in class this Summer is a perfect example of how to properly protect yourself from harm. On the plus side, technology has enabled human society to gather data much faster with much less time. We can get from point A to point B really quickly with transportation. We can reach out to anyone in the world with just a few taps on our smartphones, and with don’t even need to carry credit cards in a lot places nowadays to pay for things. Since technology is booming, white hat hackers can leverage the power of AI to aid in the process of defense. Of course, the way technology works isn’t perfect and there will always be loop holes waiting to be found by hackers. That is why white hat hackers will always be needed to keep the balance between good and evil in the cyberspace.**