Comp H

Comp H

Describe current information technologies and best practices relating to the preservation, integrity and security of data, records, and information.

Interpretation

Current technological trends have made information traveling speeds significant faster, and because of it we have been able to send information pretty much everywhere. Technologies like cloud, social media, and localhost programs for video game servers have been made stronger in the 21st century. All of these ideas sound wonderful and full of opportunity.

I remember growing up with the development of the early internet and all of the communication I had with my friend when playing video games, using Hotmail, instant messenger programs, and even the early social media platforms such as myspace. What I found fascinating about video game culture vs social media culture was the difference in security measures they applied. In 2008, Blizzard entertainment introduced a security option called an authenticator which was an external device you activated to gain access to your games associated with their company. Facebook had security measures similar to that, but the programs available were primarily third party and not officially endorsed by Facebook.

In one of my previous competencies I mentioned a conversation about accessibility vs. security. In this competency I will be talking primarily about security because it is an element that is significantly undervalued and often disregarded until it is too late. It also comes with costs which makes organizations uncomfortable because they must consider the costs and the change that come with it. The technology that I was initially skeptical with but found to be resourceful is the temporary benefits of cloud technology. While Cloud is not a very secure format and it is seen as a cheap alternative to physical storage, it at least can be beneficial when serving as temporary backup for many physical servers that fail due to external risk factors. Out of all the recent technological platforms that are being worked on right now, cloud has been working to cover their flaws including security which has been a primary concern of the platform.

Evidence

MARA 284 Cryptology Paper

We know that taking security measures is vital in the information proliferation century. I wrote a paper that talked about the evolution of cryptology and the development of secure and codebreaking techniques for dealing with locked out systems that must have involved subterfuge. You can argue that the best defense is a good offense and one the best examples in history comes from the fascinating tale of Alan Turing who broke the German enigma code of WWII. It is significant to know your enemy rather than ignore them.

MARA 284 Discussion 7

In this discussion, we talked about the significance of security alerts. Like everything in this class there is a balance to be had in the development of security protocols. There was one example where we talked about the possibility of having too much security. This is generated in the form of overflowing the system

with security alerts by generating multiple false flags to distract inexperienced security monitors into disabling them until a more severe risk accidently gets through. Having a focused and calm response to a rapidly changing scenario reduces the likelihood of a calamitous event.

MARA 249

This was a Powerpoint presentation about the Yahoo breach that was reported in 2016 but occurred much earlier. I mentioned that I was familiar with three platforms growing up and those were: cloud, social media, and email platforms. While I knew that social media was going to be breached because of the lax attitude of security measures, I did not expect Yahoo to be breached the way it was and it increased my awareness of what I posted on Facebook. Security measures seems to only be relevant after a disaster happens.

Conclusion

In the conversation between accessibility and security we have witnessed both negative extremes regarding both sides of the issue. Facebook's breach of 2017 was a lax of security and Enron's spoliation attempt was a lax in accessibility to their financial records. Security measures are important, and companies need to reevaluate their policies if they are to be prepared. Scamming calls and virus probes into corporate servers are increasing at the rate that information is developing. People assume that archivists may not have much influence in the company when it comes to security measures, but one of biggest security risks is misinformation and assuming that an archivist cannot help in security measures is a mistake. Our job is to develop organizational plans and clarity for a company so that they can focus their security teams on external threats rather than internal ones.