Miles Anderson

December 10, 2023

Why I Think Cyber Security Isn't Enough

As of 2023, technology has come an extremely long way and continues to become more and more advanced. While it's hard to imagine what technology will be capable of in ten years, it's also scary to think about what new cyber threats will arise from advancing technology. The current ethics, workplace deviance, and the short arm of predictive knowledge present in today's cyber world will not be enough to handle the new cyber threats tens years from today.

Ethics: Digitalizing DNA

When it comes to ethics in cyber security, it's important to have rules and regulations in order to protect the rights of humans. It isn't fair or morally right to cross the boundaries of another person in illegal or inhumane ways. However, when it comes to cyber criminals, they are not bound by the limits of the laws or morality. They can use technology in whatever ways they please, which is what makes them particularly dangerous. In the future, it is very possible that cybersecurity professionals will be too limited by ethics to reach the true potential of their technology. In regards to the BioCybersecuirty section of this course, I resonated with and found one article related to ethics particularly interesting. Based on my readings from the article, "Hacking Humans: Protecting Our DNA From Cybercriminals", written by Juliette Rizkallah, I

think ethical standards should be carefully considered when it comes to digitizing human DNA. Although the information can be very useful in regards to curing deadly diseases, digitalizing DNA is taking some of the most private information about an individual and making it susceptible to hackers, dark web users, and other cyber criminals. I think there should be some form of limit as to how far cyber security researchers can test on humans and how much of their personal information can be used to collect data. If an individual's DNA was compromised, it would be very hard or impossible for them to recover that stolen identity. The article also mentioned a scenario where an employer's DNA may be analyzed to determine if they are genetically fit for a job role. I don't believe this would be ethically correct because it could easily lead to discrimination in the workplace. Employers should be judged on their results on the job rather than their genetic coding. I also believe that analyzing DNA would not accurately display an individual's potential and would greatly underestimate their assets to a company. This is only one example of cyber security professionals being limited by ethics. Ten years from now, I strongly believe it will be hard to compete with cyber criminals who can use advanced technology and can operate with no rules or limits.

Workplace Deviance

Workplace deviance is another example of how cyber security professionals will struggle to keep up with cyber criminals in the future. In fact, advancing cyber technology has resulted in more opportunities for workplace deviance to occur. Typically, classified information in a workplace is restricted and inaccessible to the average employee. However, the use of malicious software can be used to hack and retrieve data without the required authorization from a higher-up. Ill-natured employees can find ways to bypass firewalls and other cyber defenses

using cyber technology in order to cause harm to an organization from the inside-out. In addition, individuals rely on advanced technology to complete tasks for them. There is less focus on human engineering and employee vetting when humans have computers to complete automated tasks. In many cases, suspicious activity performed by employees likely goes overlooked more often than it did in the past. Similarly, cyber technology has become so advanced that computers are replacing hard working individuals. In the past few years, people have been losing jobs to artificial intelligence at an increasing rate. According to O'Sullivan from tech.co, it is predicted that A.I. will replace 2.4 million jobs by the year 2030 (2023). These instances will likely motivate workplace deviance. For example, a person being replaced by a machine in their workplace may feel betrayed and bitter towards their former company. This may encourage their desire for revenge against the business, influencing them to go behind their back and cause the organization financial harm. In the age of advanced technology 10 years from now, the opportunities for workplace deviance will be bountiful and even harder to defend against. Companies will have to place extra emphasis on employee training and defenses in order to avoid losses.

The Short Arm of Predictive Knowledge

Finally, the limitless possibilities of technology ten years from now will make the short arm of predictive knowledge even more unreliable.The use of predictive knowledge can be a double edged sword in a sense. Placing too much trust in predictive knowledge and overestimating a potential cyber threat can be counter productive against developing a secure cyber policy. Making defenses for cyber attacks that are unlikely to occur can put too much emphasis on specific resources and functions which in turn may neglect the more simpler and

essential aspects of cyber defense and risk management. On the other hand, using predictive knowledge can be a great tool to learn from past instances. For example, looking at statistics of the most common cyber attacks from this year can be a great starting point on what defenses need to be implemented first. Depending on what the most common attacks are, defenses can be put in place to directly counter them. Then, policy makers can work towards the more specific and finer details of cyber defense to accommodate for unpredictable cyber attacks that may not be listed on statistics data. Overall, I believe the most important thing to do when approaching any type of cyber threat is to catch it early and react quickly. Predictive knowledge can only get policy makers so far, which is why cyber security professionals need to be prepared to react to any situation. Unfortunately, I have doubts on how useful predictive knowledge will be against cyber crime ten years from now. Through the use of artificial intelligence, some of the cyber attacks available in the future have been predicted. For instance, A.I. has predicted the use of quantum computers to surge an age of quantum based cyber attacks capable of completely bypassing encryption methods (“Futurespective 2033: cyber…”, 2023). The thought of encryption being completely useless to cyber security professionals is a terrifying possibility. The use of A.I. to strengthen predictive knowledge is invaluable, but even though knowledge of this occurrence can help prepare for it, it doesn’t necessarily mean it can be stopped. It is likely the potential of technology in ten years will be so complex that even A.I. will be unable to predict some of the new cyber crimes.

Conclusion

Cyber security is amazing, and the way professionals have defended and continue to defend against various cyber threats is nothing short of genius. Nevertheless, I don't think today’s

cyber security methods and policies will be enough to defend against cyber attacks ten years from now. Granted, cyber security will gain new tools and possibilities from advanced technology in the future the same way cyber criminals will. Many of the new threats that will arise from advanced technology will have direct counters used by professionals and ethical hackers. However, cyber security is limited by ethics, thwarted by workplace deviance, and will be left too vulnerable due to reliance on predictive knowledge to keep up with advanced cyber threats. I believe the main concept that makes cyber criminals ten years from now so frightening is the fact that we have next to no idea of what they will be truly capable of. Along with technology, criminals will likely evolve in regards to their brutality, underhanded tactics, and lack of empathy for others. I fear that one day it will be apparent how much power cyber criminals truly have over the rest of the world.

References

Futurespective 2033: cyber threats in 10 years, according to AI. (2023, Jul. 18). Nordlayer. https://nordlayer.com/blog/futurespective-2033-cyberthreats/.

O'Sullivan, Isobel. (2023, Sep. 8). *Report: AI Will Replace 2.4 Million US Jobs by 2030.* Tech.co. https://tech.co/news/ai-replace-miilions-roles.

Rizkallah, Juliette. (2019, Nov. 29). *Hacking Humans: Protecting Our DNA From Cybercriminals.* Forbes. https://www.forbes.com/sites/forbestechcouncil/2018/11/29/hacking-humans-protecting-our-dna-from-cybercriminals/?sh=16467f2a5287.