

Analytical Paper

CYSE200T

Vincent Vuocolo

Introduction

With the ever-steady growth of human advancements comes an equally steady growth in cyber-related technology. Advancements and growth of interconnected cyber-devices can be seen as a double-edged sword in a sense. On one hand, these devices have been able to connect more people together, make the world safer, make us smarter, and make our operations/infrastructures more efficient. On the other hand, these devices can be used to hack, bully, harass and overall negate the positives of the devices.

Cybersecurity is the term coined to stop such adverse effects of these devices. To ensure the safety of our users, data, and operations of cyber-devices, cybersecurity practices must be implemented. The interesting thing about cybersecurity itself is that it is a broad horizon of disciplines. One must look at the technical sides of cybersecurity and not neglect the others e.g. the social and legal aspects of the field.

With cyber tech constantly changing, the ways in which cyber devices are used for harm and how to protect them are changing. These devices have been recently found to attack small businesses and for things such as cyberstalking and cyberharassment. On the flip side, crime and deviance like these have called for an increasing need for cybersecurity-related technical systems and an overall change in how we approach the handling of such cybercrimes.

Small Businesses

Almost every company around the world has some type of cyber-tech implemented into their operations. With this being said, the risk of these businesses being attacked has gone up exponentially. User data, money, business operations in general, etc are all at risk if these network devices are not secure to a certain standard. No matter the size of the company or the wealth of the company, nobody is 100% safe from cyberattacks, Nobody.

Though being small and maybe not as wealthy as big corporations, one would think that small businesses would be excluded from a hacker's scope. This is actually far from true. A survey conducted by AdvisorSmith, a business resource company, found that out of the 1,122 businesses surveyed, nearly 50% of them experience a cyberattack(Chen). This survey only

covered a small portion of small businesses in the U.S; one could only speculate how many more of these small businesses get attacked every year.

Though small businesses are not the most targeted group by cybercriminals, the likelihood of getting attacked is still prevalent. In most companies, the need for an internal security team and or third party organization to deal with cybersecurity concerns is a must. The problem with small businesses though, is that the cost of a standalone cybersecurity team or firm may be too much to have. A study from Deloitte, an industry service provider, found that companies tend up to 15% of their IT spending on cybersecurity(Desiree). Though this may seem relatively small, these costs have the chance to add up to a lot. Having cybersecurity professionals within a small business would most likely decrease the likelihood of cyberattacks having full effects, but the cost of these professionals may outweigh the actual need for them. Though I am not downplaying the factors cybersecurity professionals play in protecting businesses, I think that the presence of one can be outweighed by security awareness training amongst associates as well as keeping the bare minimum safeguards needed to protect the company's system and assets. If I were to implement a cybersecurity change in my small business I would first assess my risk factors while cross-examining the critical infrastructures within my company. Understanding the most important assets and understanding the vulnerabilities and threats against them is step one. Let's say in this scenario I did this with my management team at a minimal cost. Next is the actual implementation of safeguards to protect my infrastructure and assets. I would start with buffing up my system's security with a firewall, and IPS, and assigning certain allowed functions amongst the associates. The cost for maintaining the IPS and firewall may be up there in cost but is worth it in the long run. My next step would be associate training in security awareness. An article from Small Business Innovative Research and Small Business Technology Transfer about the impact of cybersecurity amongst small businesses states that a frequent vulnerability amongst the businesses was email attacks(2). Training associates to be aware of attacks like phishing emails, links, etc would decrease the chance of an attack from happening in the first place. This training shouldn't cost that much because you really mostly pay for the time the associates are doing the training. Though these are only some of the changes that I would implement, they are some things that I would start at.

Cyberstalking and Harassment

Another issue that has arisen with the boom in cyber-technology and network applications in general has been the acts of Cyber-Stalking(CS) and Cyber-harassment(CH). As stated early, these cyber devices have opened a new medium for cyber-criminals and cyber-deviants to commit such cybercrimes and deviance. Marshall University defined Cyber-stalking as “the use of the Internet, e-mail, or other telecommunication technologies to harass or stalk another person”(“Cyberstalking”). Cyber-harrasment on the other hand was defined by Steven D. Hazelwood and Sara Koon-Magnin of the Univerity of South Alabama as “engaging in an act or behavior that torments, annoys, terrorizes, offends, or threatens an individual via email, instant messages, or other means with intention of harming that person”(3).

Though the use of cyber-tech for CH and CS is somewhat new, the strides to stop it has relatively been shortcoming. In the same Journal in which Hazelwood and Koon-Magnin defined cyber-harassment, they also found some of the ways local and state governments are trying to stop the acts of cyber-harassment and cyber-stalking. The journal touches on the certain legislation some states have regarding CH and CS. They describe some states as having decent legislation with “Other states still have substantial gaps in the creation and implementation of legislation that fills the cracks created by the incorporation of the Internet into everyday life.”(Hazelwood and Koon-Magnin 13)

My view on the topic is that rather than the government making all of the moves to stop CH and CS, I think the application providers themselves should step up to do a better job at stopping it. The Journal from Hazelwood and Koon-Magnin only really touches on the legislation behind the acts of CH and CS rather than legislation regarding the application providers. This may be due to the fact that there are no legislations regarding the social media platforms' role in CH and CS. Though platforms like Twitter, Instagram, Tik Tok, etc all have report/block features in their apps, CS and CH still prove to be a problem. Even if this feature proves to be overall effective, some cyber stalkers and cyber harassers will end up slipping through the crack to cause harm. Though I think the social media platforms should also be held accountable, after sitting on the idea for a little, I think it is really harder to enforce truly effective anti-CH and anti-CS policies and features than I may be portraying it to be. Let me explain. With the boom in social media, data rights issues have also become a tricky topic that

companies, legislators, users, etc have had to deal with. In my opinion, the real way to stop CH and CS is to create data profiles on each user and monitor users based on posts, chats, etc. This could help pinpoint patterns, and frequent offenders, and use such data to help prevent future harassment and stalking. This could also be used alongside the government to enforce punishment on offenders and help legislators make better laws regarding CH and SC. Though this may prove to stop CH and CS, it still seems like the platforms would be acting like “big brother” like the totalitarian rulers in George Orwell's *1984* with the platforms watching the user's every move. This approach would also most likely cross the line of the user's actual data “privacy” online. I would have to do extensive research to analyze the specific data privacy laws, regulations, and social media user agreements to really see if the approach would work.

In the end, I think that we are slowly moving in the right direction in stopping such crimes on the internet. Whether it is the government making legislation or the social media platform companies offering more tools to stop it, it is still progress in stopping such acts. As I stated previously, stopping such acts doesn't just mean preventing them strictly on a technical level, it also means studying the societal, behavioral, and legal aspects. Only this way can we truly move forward to stop things like CS and CH.

Conclusion

In conclusion, I stand by my point that there are always going to be positive and negative things that come with the growth of cyber-technology. There are always going to be cybercriminals and deviants that use this tech to hack, bully, stalk, extort, etc. It is really up to everyone, not just cybersecurity professionals, to promote the safe and beneficial use of our cyber-related devices. The fact that cybersecurity has such a broad spectrum of disciplines makes it so useful in both a technical and non-technical way. This in itself proves that cybersecurity is more than just understanding network security, malware, etc. With this being said, the growth of cyber-tech is going to keep this game of cat and mouse between cybercriminals and those who use cyber-tech for good everlasting. The only way we win this game is if we look at it through all lenses technical or non-technical, legal or societal, the list goes on.

Work Cited

1. Chen, Patrick. "Small Business Cybersecurity Statistics: 42% Attacked in Last Year." *AdvisorSmith*, AdvisorSmith, 2021,
<https://advisorsmith.com/data/small-business-cybersecurity-statistics/>.
2. Hazelwood, Steven D, and Sarah Koon-Magnin. *Cyber Stalking and Cyber Harassment Legislation in the United States: A Qualitative Analysis*, vol. 7, no. 2, 2013, pp. 1–14.
3. Macy, Desiree. "How Much Do Companies Spend on Cybersecurity?" *Security Forward*, Security Forward, 30 Nov. 2021,
<https://www.securityforward.com/how-much-do-companies-spend-on-cybersecurity/>.
4. SBIR, and STTR. "Course 10, Tutorial 1 the Impact of Cybersecurity on Small ..."
COURSE 10 CYBERSECURITY FOR SMALL BUSINESS, SBIR STTR,
<https://www.sbir.gov/sites/all/themes/sbir/dawnbreaker/img/documents/Course10-Tutorial11.pdf>.
5. University, Marshall. "Cyberstalking." *Womens Gender Center*,
<https://www.marshall.edu/wcenter/stalking/cyberstalking/>.