Marlowe Cosby

Professor Porcher

WCS 494

10/5/2022

Proposal

We are certainly aware of the issue at hand regarding hackers, cybercrime, fraud, and activities of this nature in our society today. But are we generally able, aware enough to continue to withstand these types of incidents? Sooner or later, most likely sooner, these cyber-attacks will continue to grow stronger, faster, and be more impactful than ever. The main issue at hand though isn't the cybercrime itself, but the way generally people, organizations, and companies respond to these attacks. There is already a large skill gap in the field of technology, which then increases even more once you get into the field of cyber security. Along with the skill gaps, comes the gaps in awareness as well, by those who don't need or have these technical skills. Even though everyone doesn't need a great range of technical skill, there definitely is room for minimum required knowledge of how to properly protect oneself when treading online. This is something that has been needed for some time now and yet we still see a rise in the same forms of cyber-attacks.

Former IBM chairman, president and CEO Ginni Rometty stated “Cybercrime is the greatest threat to every company in the world” back in 2015. Leap forward a few years to 2021, we saw record breaking hacks take place, creating countless issues for many, Rometty's quote did more than become true, it surpassed it. According to IBM’s 2021 Cost of a Data Breach Report, the total average cost of a ransomware attack was $4.62 million, while the average cost of a data breach was $4.24 million (IBM). The US Treasury Department found that the average amount of reported ransomware transactions per month in 2021 was $102.3 million (U.S. Department of the Treasury). As if those numbers aren’t staggering enough, the Identity Theft Resource Center’s (ITRC) data breach analysis showed that there were 1,291 data breaches through September 2021. This number indicates a 17% increase in data breaches since 2020 (ITRC). While these numbers are increasing and hacks are costing people, the economy, and business more and more, this isn’t even the main issue. What is at the root of all these attacks, breaches, and cybercrimes, is nothing but a look in the mirror.

About 95% of cybersecurity breaches are due to human error (Tuorinsky), which is where that skill gap, and awareness gap truly show to be an issue for everyone. Korn Ferry, one of the best executive recruitment firms in America, recently have been awarded 5 consecutive years of being Forbes number one ranked recruiting firm. Korn Ferry’s data reports that more than 85 million jobs could go unfilled because there aren’t enough skilled people to take them., resulting in $8.452 trillion in unrealized revenue globally by 2030 (Franzino). While not all of these are specifically tech, the majority are technology related, and along those lines of internet security it only increases (Lodewick.) Not to mention, here in the U.S. we were hit by an unprecedented

rise in cybercrime in 2021, with nearly 850,000 reports to the FBI and losses surpassing $6.9 billion in losses (Skiba). This is more than a problem at hand, as technology only becomes more complex, and at the same time integrated with daily life, we need to make a change for the greater good and protect ourselves better before it is too late.

For example, in Iran, there is currently a war between the citizens of its country and the government, but this war includes cyber warfare, as the government is shutting down their access to the internet in an attempt to keep them from spreading word of the violence happening in their country (Burgess). We are gaining information about the matter from technical specialists in Iran who are able to break through firewalls, and the governments attempt to limit access to internet and media. Without the few technical skilled people they have we may not know as much as we currently do. Clearly, we aren't there but this is just an example of what some scenarios could end up like in the future and we won't have enough technically sound people to respond. It has also raised the question of future warfare in general leaning towards cybercrimes, but that is for another day.

While I am aware I cannot single handedly make an immediate impactful change to the matter because of how large and complex of one it is, what I can do is start small and in my community with the people, organizations, and businesses around me. And hitting the main issue on the head, our own selves. With goals of increasing from my community, to the state, and so forth onto larger platforms. I aim to create an educational cyber security awareness and technical skill consulting firm that hosts workshops, create books, and media lessons to share with the public on how to better tread online safely and how to prevent, respond to these attacks. I expect to be confronted with the long tedious planning process of creating a workshop, book, in response to not only cybercrimes, and attacks, but also include valuable awareness skills to use when online. This will also take the staffing of very skilled people who are proficient in the fields of cyber security and IT.

I will know I am successful by the results of my consumers. From looking at their data, to see if attacks are going down, less cybercrime incidents occurring, and have a general technical analysis of risks, and vulnerabilities in all clients. This data will not be hard to calculate but it will take time to form and get results, as we would have to monitor and provision many technological devices and stay in contact with many people. We can search for clients by looking up recent cyber-attacks on businesses, as small businesses are actually attacked more frequently than large companies and organizations because they don't have the typical technical power to defend against most attacks (Segal). Also, I am sure with the issue being so large currently, especially the time we are in, there are many people who could use our help, and searching for clients most likely won't be that necessary. As long as we advertise properly people should come rolling in. Currently 42% of small businesses have no cyber-attack response plan (Reed), which is extremely alarming and a wide-open market for this business to thrive. We would charge by the hour if it were a consultation meeting, have a set price per workshop, have a set price for scheduled routine provisioning, and a set price per book as well. While some firms do exist in the market, nearly not enough, there are only about 3,500 cybersecurity companies in the US (CyberDB), and not enough firms to have a true count. Plus, those companies won't offer the

same things we do, they essentially come in and install their software and manage it all, or come in and clean up the mess, the attacks, and leave.

What truly sets this business apart is the connection, and teachings at hand. We would be more of a continued relationship that actually teaches people, businesses, and organizations how to properly operate. Rather than giving a man a fish to eat, we are giving him a rod and teaching him how to do it alone. Also, technology never stops growing and evolving so there will always be something new to defend against and new skills to equip and learn. Therefore this business will thrive for many years to come, and help many people in the process, and help assist the economy as well.

Works cited

Burgess, Matt. “Iran's Internet Shutdown Hides a Deadly Crackdown.” *Iran’s Internet Shutdown Hides a Deadly Crackdown*, WIRED, 23 Sept. 2022, https://www.wired.com/story/iran-protests-2022-internet-shutdown-whatsapp/.

IBM. “Cost of a Data Breach 2022.” *IBM*, https://www.ibm.com/reports/data-breach.

Franzino, Michael. “The $8.5 Trillion Talent Shortage.” *The $8.5 Trillion Talent Shortage*, Korn Ferry, 26 July 2021, https://www.kornferry.com/insights/this-week-in-leadership/talent-crunch-future-of-work.

“Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises.” *Identity Theft Resource Center*, ITRC, 21 Jan. 2022, https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/.

Lodewick, Colin. “Tech Skill Gaps Are Decimating the Global Workforce and Could Put Workers-and-Companies in Crisis.” *Tech Skill Gaps Are Decimating the Global Workforce and Could Put Workers—and Companies—in Crisis*, Fortune, 11 Mar. 2022, https://fortune.com/2022/01/28/workers-are-grappling-with-a-major-tech-skills-gap/.

Reed, Catherine. *23 Small Business Cybersecurity Statistics – 2022*, Firewall Times, 13 June 2022, https://firewalltimes.com/small-business-cybersecurity-statistics/.

Segal, Edward. “Small Businesses Are More Frequent Targets of Cyberattacks than Larger Companies: New Report.” *Small Businesses Are More Frequent Targets Of Cyberattacks Than Larger Companies: New Report*, Forbes Magazine, 24 Mar. 2022, https://www.forbes.com/sites/edwardsegal/2022/03/30/cyber-criminals/?sh=71e3b70a52ae.

Skiba, Katherine. “FBI: Nearly $7 Billion Lost to Cybercrime in 2021.” *FBI: Nearly $7 Billion Lost to Cybercrime in 2021*, AARP, 22 Mar. 2022, https://www.aarp.org/money/scams-fraud/info-2022/fbi-internet-crime-report.html.

U.S. Department of the Treasury. “Treasury Continues Campaign to Combat Ransomware as Part of Whole-of-Government Effort.” *U.S. Department of the Treasury*, 15 Oct. 2021, https://home.treasury.gov/news/press-releases/jy0410.

Tuorinsky, Edward. “Council Post: Compliance Score Alone Won't Keep Your Company Safe from Data Breaches.” *Forbes*, Forbes Magazine, 21 Apr. 2022, https://www.forbes.com/sites/forbesbusinesscouncil/2021/10/08/compliance-score-alone-wont-keep-your-company-safe-from-data-breaches/?sh=7a12657e47a9+https%3A%2F%2Fwww.aarp.org%2Fmoney%2Fscams-fraud%2Finfo-2022%2Ffbi-internet-crime-report.html+https%3A%2F%2Ffortune.com%2F2022%2F01%2F28%2Fworkers-are-grappling-with-a-major-tech-skills-

gap%2F+https%3A%2F%2Fwww.kornferry.com%2Finsights%2Fthis-week-in-leadership%2Ftalent-crunch-future-of-work+https%3A%2F%2Fwww.forbes.com%2Fsites%2Fedwardsegal%2F2022%2F03%2F30%2Fcyber-criminals%2F%3Fsh#:~:text=CyberDB%20is%20the%20perfect%20place,3%2C500%20US%20cyber%20security%20vendors.

"USA Cyber Security Companies." *CyberDB*, 7 May 2018, https://www.cyberdb.co/database/usa/#:~:text=CyberDB%20is%20the%20perfect%20place,3%2C500%20US%20cyber%20security%20vendors.