Why You Should Consider Learning Cybersecurity

3.12 million. This is the estimated number of cybersecurity specialists needed globally as cyberattacks around the world keep growing in both frequency and magnitude (Duffy, 2021). The last few months alone have seen some of the biggest security breaches in history, more on which later. The most important development in the cybersecurity narrative recently is that the latest high-profile cases have gone outside of the scope of customers' private data leakages, which we have frankly got used to already. Instead, the US gas distributor Colonial Pipeline and one of the world's largest meat producers JBS paid a combined sum of more than $15 mln to hackers in a matter of a few days in order to get their operations back to normal after a forced halt because the hackers had gained full access and control over their online systems (Wood, 2021) (Fung, 2021). These instances represent a different form of cyberattack, one that hinders our everyday life in ways that data leakages, though dangerous and scary, never could. Gas shortages along the East Coast of the US, where Colonial mainly operates, are but one of the consequences of a general trend of disruptions due to cyberattacks. Hence the urgent need for cybersecurity professionals, fueled also by the rapid, forced, and completely unprepared digitalization of business operations around the world due to the pandemic.

When the world stopped for a while as we were forced to stay home last year, anything that could go online, did so. While the most famous companies such as tech-giants Facebook or Google were quick to adapt and had a relatively easy shift to the online world, not all companies were as well prepared or had all the necessary conditions to smoothly transition to the work-from-home format. That haphazard transition meant cybersecurity was sometimes neglected in order to keep the company going. Without any preparation or training, employees began working online,

precious private information and documents were digitized and stored on online platforms or clouds and too little attention was paid to the security of those systems. This did provide a lifeline for many companies and their employees during the most severe times of the pandemic, but it also opened the door wide for cyberattacks.

In May, the aforementioned Colonial Pipeline fell victim to a ransomware attack, one that blocks the company's access to its files and systems, which can only be accessed again if the company pays a ransom to the attackers. It eventually had to do exactly that: the company paid $4.4 mln, a decision their CEO says was made hours after the attack had occurred (Olenick, 2021). JBS had to be even more generous and had to pay $11 mln. From the companies' point of view, paying the ransom was probably the most optimal decision it could have made.

The companies did not have many options. Essentially, it came down to the choice between paying the ransom or not. As economists like to point out, a rational agent makes a decision based on the marginal benefits and marginal costs of the alternatives. While the management might realize the mistake of underinvestment in cybersecurity in the past, that mistake has already been made and none of the current alternatives can change that. So, when faced with the choice of either restarting their operations or having to endure an indefinite freeze without an action plan of how to restore life back to normal, the benefits of being able to work again far outweigh the millions of dollars that the hackers demand. In the grand scheme of things, though, such actions by the victim company may serve as an incentive for the ransomware attacks to grow and multiply, but that is not part of the company's decision-making process. So as long as cybersecurity is not at a far more advanced level everywhere, ransomware attacks will be directed against companies that never suspected they could be targeted, and most of the time, the attackers will get what they want.

Property rights have been an indispensable part of human existence for as long as there is recorded history of it. For the vast majority of that time though, the definition of property included physical, tangible assets, ones that can be seen, moved and stored in a safe place. While conceptually quite close, physical security and cybersecurity are, unfortunately for most companies, two completely different services that they must acquire in order for their property to be safe. As intellectual property such as the data and documents that companies store online increasingly becomes more valuable than all the tangible assets that they own, the demand for cybersecurity specialists, “bodyguards of IP”, if you will, is growing faster than for most other occupations, so whether you are considering a change of sphere or are undecided as to what you want to do with your life, a career in cybersecurity seems a good bet going forward.

References

Duffy, C. (2021). *Wanted: Millions of cybersecurity pros. Salary: Whatever you want*. Retrieved from CNN Business: https://edition.cnn.com/2021/05/28/tech/cybersecurity-labor-shortage/index.html

Fung, B. (2021). *JBS says it paid $11 million ransom after cyberattack*. Retrieved from CNN Business: https://edition.cnn.com/2021/06/09/business/jbs-cyberattack-11-million/index.html

Olenick, D. (2021). *Colonial Pipeline CEO Confirms $4.4 Million Ransom Payment*. Retrieved from Data Breach Today: https://www.databreachtoday.com/colonial-pipeline-ceo-confirms-44-million-ransom-payment-a-16696

Wood, R. W. (2021). *Colonial Pipeline Paid $4.4 Million In Bitcoin Ransom. Is It Tax Deductible?* Retrieved from Forbes: https://www.forbes.com/sites/robertwood/2021/05/20/colonial-pipeline-paid-44m-ransom-can-you-deduct-ransom-on-your-taxes/?sh=2cef06487d87