Rising Cybersecurity Tension and Ways to Prevent Future Catastrophe

Thomas Morgenstern

October 13th, 2021

Table of Contents

Abstract

There is a general lack of enforcement of security measures in the cyber industry. More specifically, there has been an increase in technology with access to the internet over the years spanning nearly every different facet of business. With the advent of nearly every new piece of technology containing some sort of software aspect, there comes the issue of cybersecurity. This issue is exacerbated by the rapidly increasing number of appliances that use software and the poorly designed economic and legal systems relating to the software development industry. The suggested solution in this proposal will discuss advocating for an increase in education to the general public and technically skilled workers through government and academia. The solution will also suggest an analysis and improvement of the standards currently in place regarding software development in the economic and legal spheres. The benefits of this proposal will fundamentally reduce the potential damage produced by malware on systems created now and in the future.

Proposal

Since the creation of micro chips with enough processing power to run decently sized systems of software, there has been an ever growing number of appliances developed in which software is incorporated into. Today, nearly every newly produced technology that is powered by electricity contains some hardware that contains embedded systems with software. "From entertainment and communications to energy, healthcare and finance, industries are increasingly 'being run on software and delivered as online services'" (Daley). The push for this is derived from the promise that with appliances being connected many tasks become automated and life becomes easier. While that is true, it is also true that those who produce these new technologies should take into consideration the well being of the end user. More specifically, not just the user experience on a surface level, but what issues may arise from negligence to produce the products correctly, and not just quickly. Particularly, these software systems embedded in these new technologies should contain well made, tested, and bug-free code; but they should also contain secure code, as well. However, the legislation and economics entwined in software development make it very unworthwhile for the software developers to provide adequate security. So, the way in which software developers consider cybersecurity, "a set of technologies and processes designed to protect computers, networks, programs and data from attack, damage, or unauthorized access," needs an update (Sarker).

An excellent example of the implications of ignoring cybersecurity issues is as follows. "*Ars Technica*… reported on Shodan, a search engine for the IoT," Internet of Things, which is a term that describes objects that use software and communicate with other objects, "that lets users easily browse vulnerable webcams. The feeds include 'images of marijuana plantations, back rooms of banks, children, kitchens, living rooms, garages, front gardens… colleges and schools, laboratories, and cash register cameras.' Most alarmingly, several feeds included sleeping children" (Daley). While the problem with unauthorized access to cameras is creepy and unsettling, it still doesn't quite capture the full potential danger that comes from ignoring producing quality technology with proper cybersecurity.

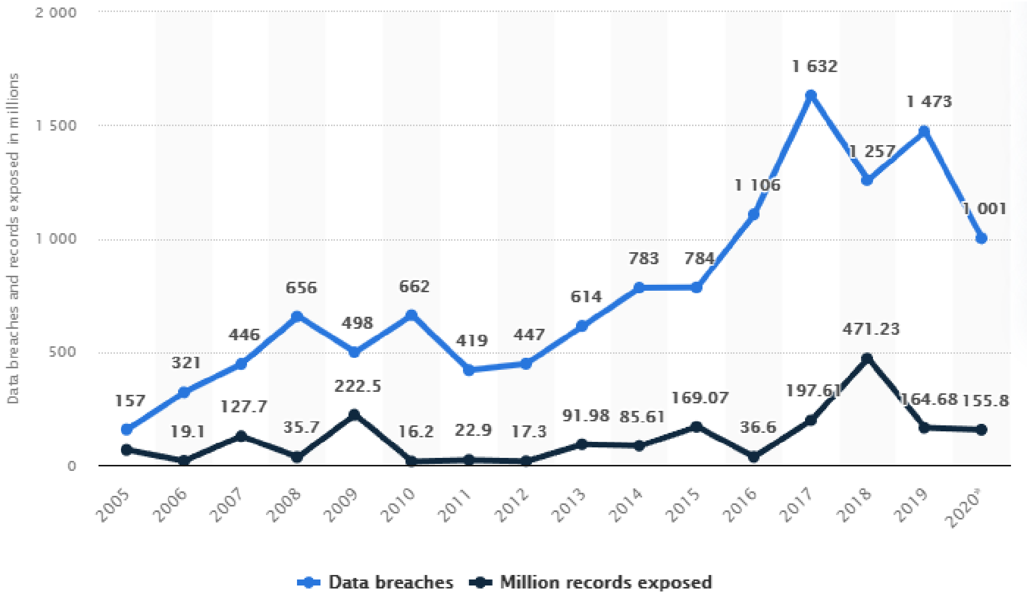

Figure 1

Throughout recent years the number of data breaches for companies in the U.S. have drastically increased. As can be seen in Figure 1, there was an all time high of 1,632 data breaches in 2017 and an all time high of 471.23 million records that were exposed in the following year. By ignoring cybersecurity, while also exponentially producing new technologies that use software and the internet, we have effectively opened ourselves up to these kinds of threats. Data breaches create incredible financial loss, produce reputational damage, and force companies to stop producing and spend costly time on recouping and taking legal action.

The first way in which the lack of cybersecurity in the engineering world should be addressed is through education. There are a few cybersecurity initiatives that have been started around the world in recent years. One in particular known as NICE, the National Initiative for Cybersecurity Education, which is "led by the National Institute of Standards and Technology

(NIST) of the U.S. Department of Commerce, [and] is a partnership between between government, academia, and the private sector working to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development" (Newhouse). This improvement and general increase in education over the general population vastly improves the quality of cybersecurity overall because it allows the general end user of some software system to evaluate the software system they're using themselves. A majority of people who use software everyday don't understand how the systems they use actually work. Therefore, by educating the general public on the best practices and red flags of cybersecurity the end users can also place stress upon the software developers to produce more quality software.

Another way in which the lack of cybersecurity in the engineering world should be addressed is through an economic and legal reevaluation of software. Currently, there is little policy that enforces the software developer to spend time producing security measures for newly created software, considering they're rarely held liable. While this fact allows for incredible innovation, it hurts the end user that is uninformed. "Some strident critics of the industry have argued that the current paradigm is exceedingly generous to developers and has permitted the software industry to 'blame cybercrime, computer intrusions, and viruses on the expertise and sophistication of third party criminals and on careless users who fail to implement adequate security, rather than acknowledging the obvious risks created by their own lack of adequate testing and flawed software design'" (Daley). A probable objection to this line of thinking is that a solution involving strict liability "would stifle software innovation and potentially erode incentives for other actors, like end users, to employ good security practices" (Daley). While this is a somewhat valid argument, there's no reason why there can't be a solution that meets somewhere in the middle. In serious debates regarding this topic, no one answer can be put forth as the best option, however logically it makes sense that "there are two approaches to improving security given these… realities: incentivising or mandating increased ex ante investment in security by developers, or increasing ex post punishment through a liability regime to compensate victims and provide discipline through deterrence" (Daley). The most appealing of the two options being incentivising the improvement of security. With an incentivised environment software developers would feel the need to produce secure software systems.

A final way in which the lack of good cybersecurity in the engineering world should be addressed is through advocating for the inclusion of data science into the security measures employed.

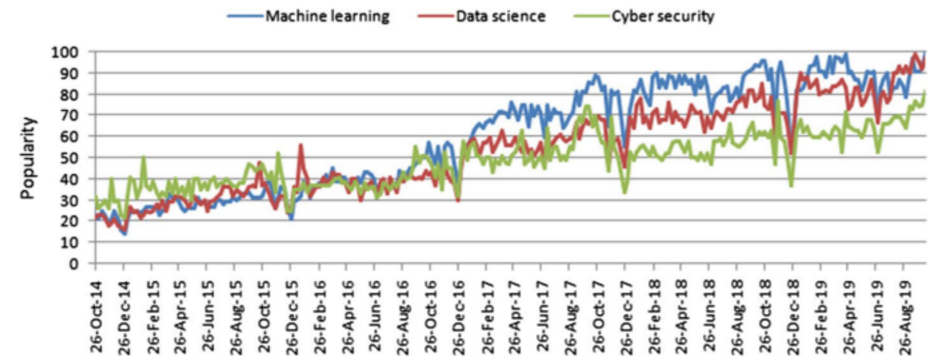

Fig. 1 Popularity trends of data science, machine learning and cybersecurity over time, where x-axis represents the timestamp information and y axis represents the corresponding popularity values

Figure 2 Recent developments relating to cybersecurity include "massive shifts in technology and its operations in the context of computing, and *data science* (DS) is driving the change, where *machine learning* (ML), a core part of *"Artificial Intelligence" (AI)* can play a vital role to discover insights from data" (Sarker). As can be seen in Figure 2, the popularity of data science, machine learning, and cyber security has increased generally over time, and with this came the focus of cybersecurity data science, "which is broadly related to these areas in terms of security data processing techniques and intelligent decision making in real-world applications" (Sarker). The purpose of data driven cybersecurity is to create security solutions that are intelligent. By collecting massive amounts of cybersecurity data, we can "address this issue… [of] develop[ing]

more flexible and efficient security mechanisms that can respond to threats and… update security policies to mitigate [attacks] in a timely manner" (Sarker). This approach to dealing with cybersecurity incidents is appealing because it handles the issue with the proper care and attention it needs. Producing proper techniques and tools to effectively combat the negative effects of cyber attacks requires the ability to analyze data and understand the numbers with a nuance that no human likely can. So, employing the help of DS/AI is the perfect solution to help try and understand the ramifications of cyber attacks.

Works Cited

Daley, John. "INSECURE SOFTWARE IS EATING THE WORLD: PROMOTING CYBERSECURITY IN AN AGE OF UBIQUITOUS SOFTWARE-EMBEDDED SYSTEMS." Stanford Technology Law Review 19.3 (2017).

Newhouse, William, et al. "National initiative for cybersecurity education (NICE) cybersecurity workforce framework." NIST special publication 800.2017 (2017): 181.

Sarker, Iqbal H., et al. "Cybersecurity data science: an overview from machine learning perspective." Journal of Big data 7.1 (2020): 1-29.

Tervoort, Tom, et al. "Solutions for mitigating Cybersecurity risks caused by legacy software in medical devices: a scoping review." IEEE Access 8 (2020): 84352-84361.

van der Linden, Dirk, and Awais Rashid. "The effect of software warranties on cybersecurity." ACM SIGSOFT Software Engineering Notes 43.4 (2019): 31-35.

Figures Cited

Figure 1

Johnson, Joseph. “U.S. Data Breaches and Exposed Records 2020.” *Statista*, 3 Mar. 2021, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

Figure 2

Sarker, Iqbal H., et al. "Cybersecurity data science: an overview from machine learning perspective." Journal of Big data 7.1 (2020): 1-29.