Securing Our Digital Future

Introduction

From IPhones to virtual reality to social networks, the ways in which people leverage technology in their day to day have only become more and more intractable. Yet, in the shadow of this growing technological dependence, lies a little digital realm that also grows. Everyday, it is more and more infiltrated, compromised, hacked, and the sad reality is that the reason it seems this way is because more corporations are getting hacked. The past couple years have been an intense prime time for cybersecurity threats, as each day a greater number of bad actors put their fingers to the keyboard in order to hack into the most secure technological systems in the world. This catalog will discuss threats to the cyber realm and how they can be mitigated.

What is Cybersecurity?

Practically, cybersecurity is the combination of cyberspace and security. It is merely every aspect of physical security - something that can exist in the real world - and translating it into a digital form. What does security accomplish? In short, it can be summed up with a common alliteration between the three C's: CIA. [2]

Confidentiality	**Items are protected from unauthorized access.**
Integrity	**Items are protected from unauthorized modifications.**
Availability	**Items should be accessible to authorized users.**

As you can see, breaking one or more of these attributes can lead to widespread problems that severely affect everyone, not just the company itself. In the following sections, we will discuss how cybersecurity can affect consumers more in depth and take a look at a few specific incidents.

The Challenge of Cybersecurity

Why is it a Problem?

Cybersecurity is incredibly important - without proper internet security, corporations can suffer data breaches and lose vital financial information. Companies often dash underneath the cybersecurity umbrella in hopes that they do realize the importance of cybersecurity in the too late and they are responding to an incident. Cybersecurity is hard to put a monetary value on because it prevention is supposed to prevent something which companies see as sinking leading to more revenue. [3]

On a personal level, companies who hold your data can suffer data breaches, and these have been known to leak constant IP addresses, emails, phone numbers, addresses, and names.

It may seem like a company's cybersecurity policies do not affect consumers as it's the company's data being lost if they get hacked, but the company owns a part of you: your data and your digital address for easy shopping, your phone number to reach you and send you marketing materials, your profile picture that has a lot of your friends in it. When you sign up for a service, you are agreeing to have companies hold onto this information and do whatever they want with it.

What Led to its Emergence?

With consumers being less willing to pay for services and more free websites, games, and apps, Companies tend to look elsewhere for their main money. That revenue comes from your data in advertisers. The Documentary Social Dilemma summarizes this best: "If you are not paying for the product, you are the product" meaning that companies will sell your data if you are not paying for their product [11]. This is an economic principle because companies need to make money in order to survive.

Technology and government laws have cut off consumers and companies from each other. Companies are incentivized to use data to less likely be sued. Recently Apple developed "App Tracking Transparency" policy which requires apps to ask permission to track users. The ability for people to opt out of tracking has caused companies like Facebook, Snapchat, Facebook, Twitter, and Google to lose around $9.85 billion in revenue following Apple's changes to its privacy practices" according to a report by The Verge. [8]

Industry Failures

50 Million

A company, Cambridge Analytica, had been known to use data from Facebook to sway elections in the United States, Nigeria, and the United Kingdom. Current industry failures around cover around data breaches. This is a very lucrative business because it is the easiest, and most people-friendly method of the breach. Currently the piece of legislation is holding companies accountable for data breaches, they are expected to report it "good faith". [7]

As right and Americans began to voyage into the blackness of their satellite, in various locations around the world, the terrified faces of 37 personnel were awash with a dim red light emanating from their monitors. Frantic shouts of "we've been compromised!" echoed over conducted. Present in these screens, standing out proudly against the computer's newly red background was an unsolicited, "ransom note" from the hacking group, WannaCry.

Though the WannaCry attack was conducted in May of 2017, the memory of it seems to be forever stuck in the minds of those who were directly enough to be affected. Unlike other cyber attacks have affected greater numbers of companies and inflicted greater amounts of damage, what made WannaCry unique was the way it spread and the ease of which the computer system around the world. With WannaCry affecting everything from hospital systems to company servers and personal devices, for the first time, it showed everyone how vulnerable society's digital systems truly are.

The Origin

As with the majority of cyberattacks, the origin of the WannaCry ransomware is quite murky. Cybersecurity experts are unsure of the damage that it caused. The reason for the worm's rapid spread would due to WannaCry being an incredibly unique and sophisticated piece of software. It's spread would be classed as a individual worm, it was being to update their devices. In April, a month before the ransomware was deployed, a previously unknown internet group called the "Shadow Brokers" leaked a cache of hacking tools. The spread, and contained within their treasure trove of hacking tools was a piece of software called EternalBlue. Put simply, EternalBlue takes advantage of a security flaw in the Windows Server Message Block protocol to execute illegal code on the machine without needing the user to do anything. Microsoft had patched the security flaw in March, but many of the hacked-before-that-patch-to-update-to-be-safe-from-hacking-tools-released-it-into-their-virus-to-it-could-spread-through-the-world-to-computer-systems-that-were-not-updated-to-the-patch-that-was-released-to-stop-the-spread-of-the-virus-that-was-released-into-the-world-through-the-hacking-tools-released-by-the-hackers-who-hacked-into-the-Shadow-Brokers-hacked-their-system-to-access-the-hacking-tools-they-released-into-the-world-to-be-used-to-hack-into-computers