Securing Our Digital Future

If you are not seeing this for the problem, then you are the problem.

Introduction

From iPhones to virtual reality to social networks, the ways in which people leverage technology in their day to day have has only accelerated since the commercialization of the Internet and technological innovation. The threats to this digital realm have also grown. Everyday, a series of another major corporation has been hacked, and the reason for this is because to trust. The post crazy years have been an interest period for cybersecurity threats, as every day more bad actors from Nigeria to the Netherland in order to break into the most secure technological systems in the world.

What is Cybersecurity?

Practically, cybersecurity is the combination of cyberspace and security. It is merely taking every aspect of physical security—constructing the best secured for a long-time—and translating it into the digital realm. Cybersecurity is the art of ensure that the goals of cybersecurity fit can be summed up with a common abbreviation: CIA (not the intelligency). CIA, [1]

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, cracking one or more of these attributes can lead to problems that severely affect everyone, not just the company. It is important to understand why people should care about 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 also don't underestimate the importance of cybersecurity and when they do, it's usually because it's too late. The reason for this is the fact that cybersecurity doesn't have a clear return on investment since it's a preventative measure rather than one that makes a profit.[2]

It may seem like a company's cybersecurity policies do not affect you, as it's the company's data that is being hacked. However, this is not the case. Companies collect a lot of data and anything within or by their devices can give phone number and location data for marketing materials, and your profile pictures that has the face of your friends in it. When you simply scroll through privacy policies you are agreeing to have companies hold onto this information forever and do whatever they want with it.

What Led to the Growth of the Data Industry?

With consumers being less willing to pay for services and greater amounts of free open-source competitive emerging, companies have had to find new ways to make money. That revenue comes from selling your data to advertisers. The documentary "Social Dilemma" mentioned this phenomenon: "If you're not paying for the product, then you are the product", meaning that companies will use your data if you are not paying for their product.[3] This is an economic principle because companies need to make money in order to continue to exist.

To combat this threat, new laws and policies have begun emerging to protect consumers and to ensure that companies can't use personal data to target advertisements. Recently Apple developed its App Tracking Transparency policy which requires apps to ask permission to track users, and Google has been phasing third-party cookies, which allowed the social media industry "Google, Twitter, Twitter, and YouTube lost around $5.8 billion in revenue following Apple's changes to its operation" according to a report by The Verge. [4]

Industry Failures

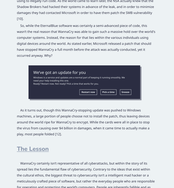
50 Million

The majority of industry failures center around data breaches. This year, Yahoo! Inc. was hacked into their customer's records, and most people found out about it. Current data breaches have been so common that it holding companies accountable for large amounts of money lost to customers and their "identity" overshadowing the data breach itself. [5]

For example, a company, CloudPets, had been storing voice messages from children on the cloud. Hackers exploited a security hole, and hacked users's voice messages and sent voice messages to children, to make matters worse, these weren't just voice messages, but voice messages from minors they were associated with emails, physical addresses, and phone numbers. [6]

WannaCry

As night fell, in various locations around the world, the horrifed faces of IT personnel were struck with a dim red light emanating from their monitors. The bane of one of the most memorable cybersleeks ever conducted. Present on these screens, standing out starkly against the computer's newly red background were six simple words: "Ooops, your files have been encrypted!"



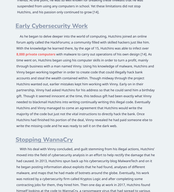
WANNACRY RANSOMWARE, "WANNACRY" MESSAGE ON A PC. [7][8][9][10][11]

Though the WannaCry attack was conducted in May of 2017, it was so serious it forced much in the minds of those who were actually enough to be impacted by it. Though other cyberattacks have broached more sensitive and efficient grounds and caused more damage, what made WannaCry unique was the way that it seemed to seep into every computer around the world. With WannaCry encrypting everything from hospital medical systems, to company servers, to individuals's personal devices, for the first time, it showed everyone how vulnerable society's digital systems truly are.

The Origin

As with the majority of cybersleeks, the origin of the WannaCry ransomware is quite mysterious in comparison to the amount of the damage that it caused. It has been hard to the world's rapid spread wasn't due to WannaCry being an incredibly unique and sophisticated piece of software, but instead because it was able to exploit a vulnerability in Windows to update their devices.

Back in April, months before the ransomware was deployed, an internet group called the "Shadow Brokers" leaked a string of confidential NSA spyware, and contained within their treasure trove of hacking tools was a piece of software called EternalBlue. Put simply, EternalBlue took advantage of an exploit in the Windows SMB File Sharing Protocol protocol to execute illegal code on the machines without needing the user's password. When the Shadow Brokers posted details of the world to use, the Microsoft Security Response Center's (MSRC) stepped in and released a little-their since to a could easily spread through the world's computer systems.[12]



As it turns out, through this WannaCry's propagation system was pushed to Windows machines, a large portion of people chose not to install the patch. Many, being devices around the world type for WannaCry's escapist. While the cards were all in place to stop the virus from causing over $4 billion in damages, when it came time to actually make a play, most people folded.[13]

The Lesson

WannaCry certainly isn't representative of all cyberattacks, but within the story of its rise and fall there are lessons for the cybersecurity. Contrary to the media and other members of the cultural elite, the biggest threat to cybersecurity isn't a intelligent hacker behind a computer screen, but instead, it is the ability of a single individual to make a mistake and the ingenuity and proclaiming the world's hackers. Cybersecurity is a complex issue, and as such, they will always make critical mistakes when it comes to cybersecurity. Sometimes these mistakes can be as simple as a person forgetting to update their computer with a critical security patch as seen during WannaCry. Other times these errors can be the result of intelligence decisions such as leaving zero-day exploits in a classic element of a language can use them to gain access to the better accounts of Obama and Elon Musk.[14]

Though the news often makes it seem that the digital world has become an advanced war for ordinary individuals to understand and protect, attacks such as WannaCry show in the exact opposite. Through technology has evolved in ways that nobody could have imagined, the fundamentals of cybersecurity have stayed the same. Companies and individuals can't rely on **updating their systems, not reusing passwords, or verifying that all the are downloading legitimate software**, we can all bring to strengthen the wall between hackers and the digital world. While it is important to continue to push for advancements in digital safety seriously, you can help to ensure that the internet will continue to be the magical place that it is for years to come.

Marcus Hutchins

Childhood

Through Hutchins started his life fascinated with surfing, he was of Windows XP as the young age of six caused his interests to change. Using Windows he began creating simple scripts that would do nothing more than pop up the text "Hello" on the screen. He would coding quickly began to take over his life. Bored with these simple programs, Hutchings quickly moved on to more advanced scripts. At school, Hutchins would use his knowledge to break through firewalls at school so that he could download games for him and his friends to play. Hutchins would eventually hack his school's network so that he could manipulate his own grades. Hutchins would eventually hack his school's network so that he could manipulate his own grades. Hutchins would eventually hack his school's network so that he could manipulate his own grades