

# BTI Education \* TLIM 4397 – Introduction to Homeland Security Project title: DHS Strategy: A Study On Combating Cyber Crimes

Student Researchers: Taylor Howard and Abdul Ladha Supervising Faculty: Prof. Maria G. Burns (BTI, CoT)

### **Purpose and Motivation:**

- Each year, thousands of cyberattacks by overseas governments, terrorist groups and transnational criminal organizations target U.S. entities.
- Because of the dependency we have on technology, we become very vulnerable to many cyber-attacks such as identity theft, breaches, ransomware, and hacking.

### **Problem Statement:**

While government entities and large organizations have the know-how and resources to fight cybercrime, many Americans and small-medium companies either lack the knowledge, or the resources (or both) to adopt proper cybersecurity protocols. This renders them vulnerable to be protected from cyber attacks. As a result, our nation experiences an increasing number of attacks, with loss of intellectual property, commercial and personal data, identity theft, but also financial and other losses.

### Research Methods and Approach:

- In this research, facts, and figures from secondary data are used to identify:
- a) Which industries are mostly attacked,
- b) How ransomware damage and costs have increased?c) Which are the top countries that are expected to be attacked more frequently?
- This project will help better understand the threats of cybersecurity, and future trends.



as y, a magnes and a second and s

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 17STBTI00001 (formerly 2015-ST-061-BSH001).

**Conclusions:** 

The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

### Research Analysis: Upon researching various reports, a new chapter in the history of Cybersecurity appears.

- Ransomware attacks doubled in 2019, per McAfee. Ransomware incidents increased by 118%. 77 percent of targeted attacks relied on user interaction.
- New malware samples have increased by 35% due to malware leading disclosed attack vectors, followed closely by hijacking and targeted attacks.

# Contribution Of Countries To World Cyberattacks Russia 4.3% Hungary 1.4% China 41% India 2.3% India 2.3% https://blog.eccu.edu/industries-that-are-most-and-least-vulnerable-to-cyberattacks/

# Most Vulnerable Targets 2019-2020

1. BANKING & FINANCIAL Institutions (400% increase (NCC, 2019-2020)

2. HEALTHCARE (32K Intrusion attacks each day)

4. ENERGY, MANUFACTURING, TRANSPORT

5. SMALL & MEDIUM Companies

### EVERY 2 SECONDS, AN AMERICAN BECOMES VICTIM OF IDENTITY THEFT **MARRIOTT HACK FACEBOOK HACK WORDS WITH FRIENDS HACK, 383 MILLION PERSONS 540 MILLION PERSONS** 218 MILLION ACCOUNTS **AMCA hack impacted HOUZZ, 49 million records CAPITAL ONE BANK** LabCorp, 7.7 million of 100 MILLION AMERICANS, 6 hacked customers' financial and **MILLION CANADIANS ZYNGA Mobile Games** health data. PERSONAL INFO,

### Sources:

**AMCA files for bankruptcy** 

- CNET, 2019 Data Breach Hall of Shame @ Identity Theft Resource Center
- · ABC NEWS @ SelfKey.org @ <u>www.idtheftcenter.org</u> @ Gartner Report 2019, 2020

218 MILLION CUSTOMERS

2019-2020: >16 BILLION RECORDS EXPOSED (Banking, Personal data)

By 2021, the annual COST OF CYBERSECURITY will exceed ~6 Trillion

In the COVID era, HEALTH DATA is 50 times more prized by Hackers

Cyber IDENTITY THEFT has impacted 60 MILLION AMERICANS

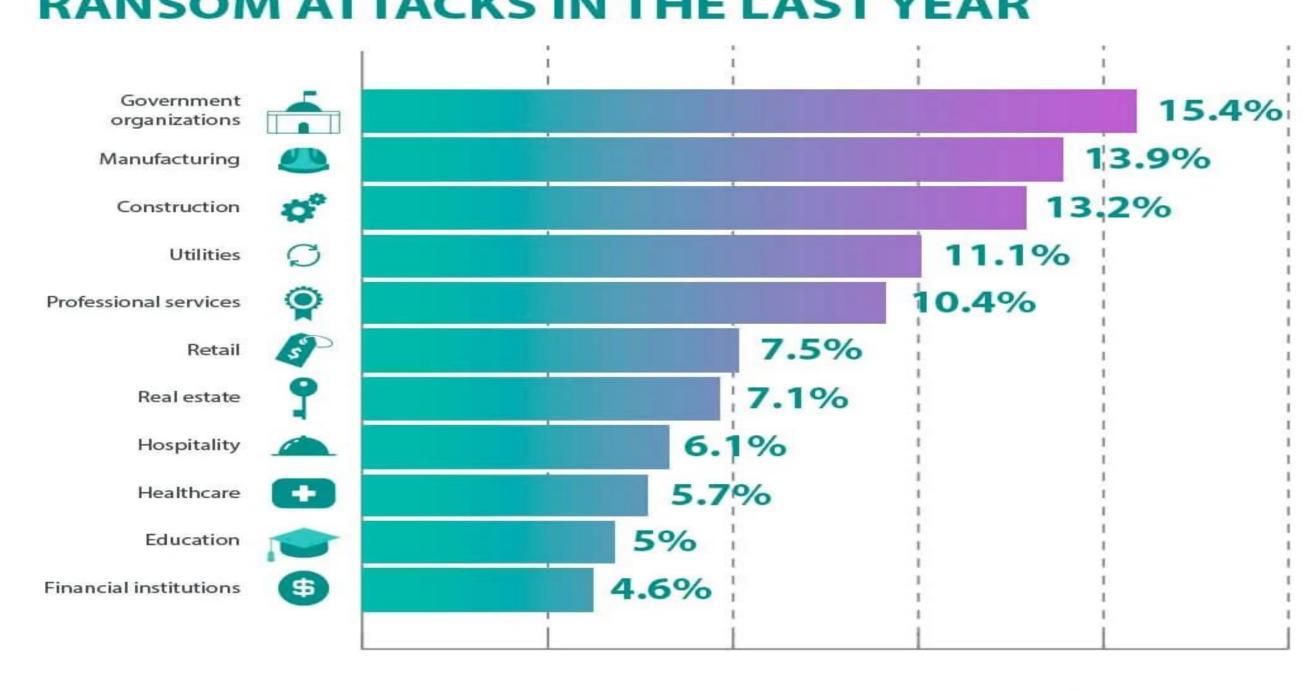
EasyJet Airlines – 9 million customers' Credit/Debit cards

Marriott Hotel → 5.2 million guests

MGM Grand Hotels, Las Vegas 10.6 million guests

**ZOOM Passwords/Login credentials sold on the Dark Web** 

# INDUSTRIES IN NORTH AMERICA REPORTING RANSOM ATTACKS IN THE LAST YEAR



### Percentage of all reported incidents caused by ransomware, as surveyed in 2019 Safety Detectives

## Upon examining government reports and official statistics, a key concern appears to be the fact that the general population is not very familiar with internet security.

We posit that if the government or educational initiatives informed more people about efficient internet practices then the percentage of vulnerability would decrease substantially, and fewer people would become victims of cyber-attacks.

### References:

- https://blog.eccu.edu/industries-that-are-most-and-least-vulnerable-to-cyberattacks/
- https://www.csoonline.com/article/3260191/security/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html
   https://www.healthcareitnews.com/news/los-angeles-provider-breached-ransomware-attack-over-260000-patients-affected-updated
- https://info.bitsight.com/the-urgency-to-treat-cybersecurity-as-a-business-decisionppc?utm\_term=cyber%20security&utm\_campaign=Risk+and+Information+Security+-+NA&utm\_source=bing&utm\_medium=ppc&hsa\_cam=6483867836&hsa\_mt=p&hsa\_ver=3&hsa\_src=o&hsa\_ad=&hsa\_net=adwords&hsa\_tgt=kwd-

84525130265441:aud-808186952:loc-4126&hsa\_acc=9761199014&hsa\_grp=1352399519825876&hsa\_kw=cyber%20security&msclkid=08072946677612dfac5d76225abb1ac0

