Consequences of Cybercrime

Like other forms of crime, cybercrime has consequences for both society and the economy. Another way of saying this is that there are both social and economic costs of cybercrime. We will start with a discussion of the societal costs of cybercrime. Although it is difficult to quantify the costs of cybercrime to society, it is possible to conceptualize such consequences. In order to understand the social consequences of cybercrime, we first have to understand that we now live in an **information society**.

From Wikipedia:

An **information society** is a society where the creation, distribution, use, integration and manipulation of information is a significant economic, political, and cultural activity. Its main drivers are digital information and communication technologies, which have resulted in an information explosion and are profoundly changing all aspects of social organization, including the economy, education, health, warfare, government and democracy. The people who have the means to partake in this form of society are sometimes called digital citizens. Information society is seen as the successor to industrial society.

An alternative definition from the Website WhatIs:

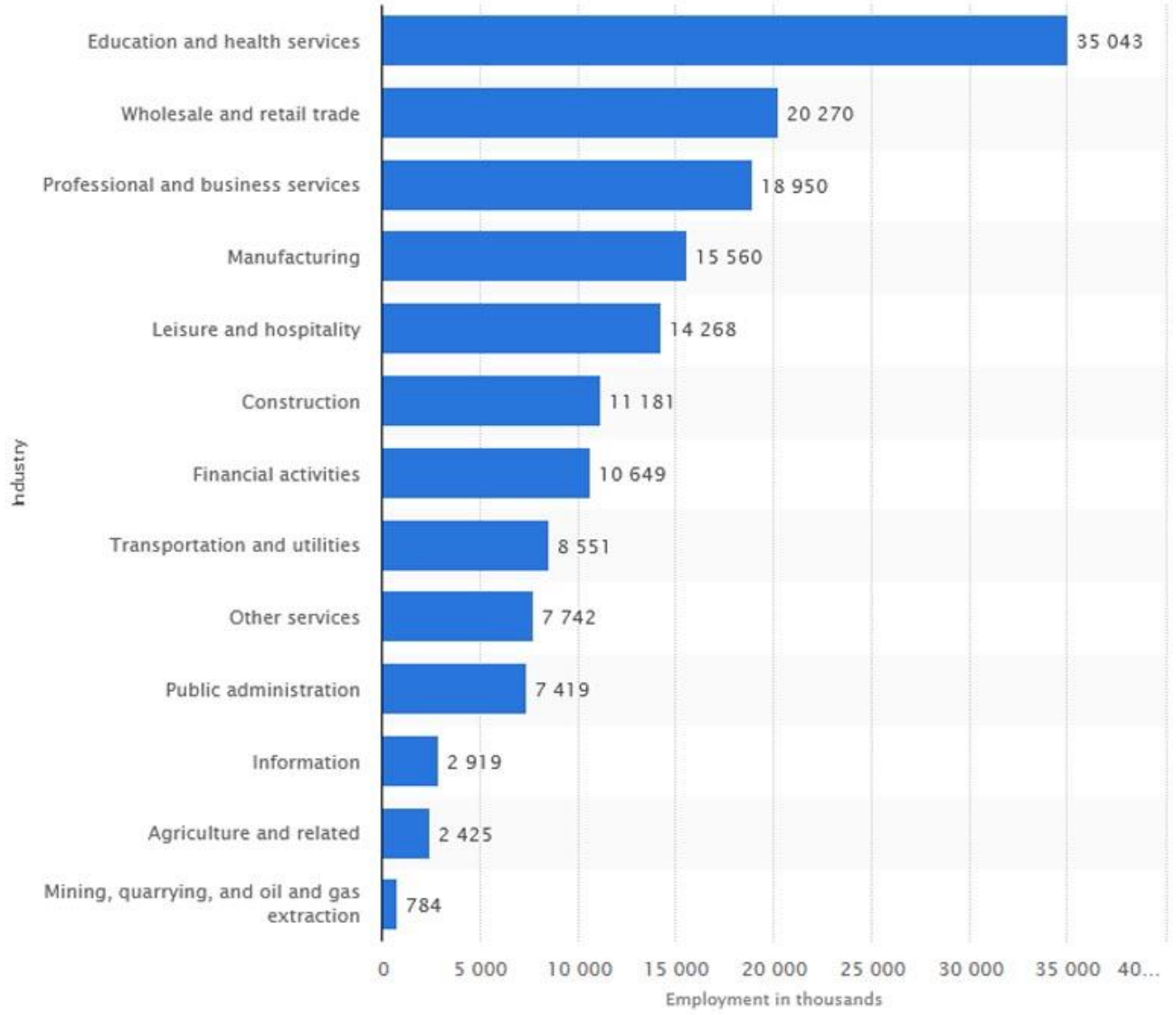
Information Society is a term for a society in which the creation, distribution, and manipulation of information has become the most significant economic and cultural activity. An Information Society may be contrasted with societies in which the economic underpinning is primarily Industrial or Agrarian. The machine tools of the Information Society are computers and telecommunications, rather than lathes or ploughs.

Policy makers for the G7, a group of economically developed nations, stated that: **Progress in information technologies and communication is changing the way we live**: how we work and do business, how we educate our children, study and do research, train ourselves, and how we are entertained. The information society is not only affecting the way people interact but it is also requiring the traditional organizational structures to be more flexible, more participatory and more decentralized. (Chair's conclusions from the G-7 Ministerial Conference on the Information Society, February 1995.)

The following slide presents data on the numbers of employees in various occupational categories in the United States in 2018.

Total employed persons in the U.S. in 2018, by industry

(in 1,000s)



Number and Percentage of Employees in Information and Other Occupational Categories- 2018 (Source: Statista)

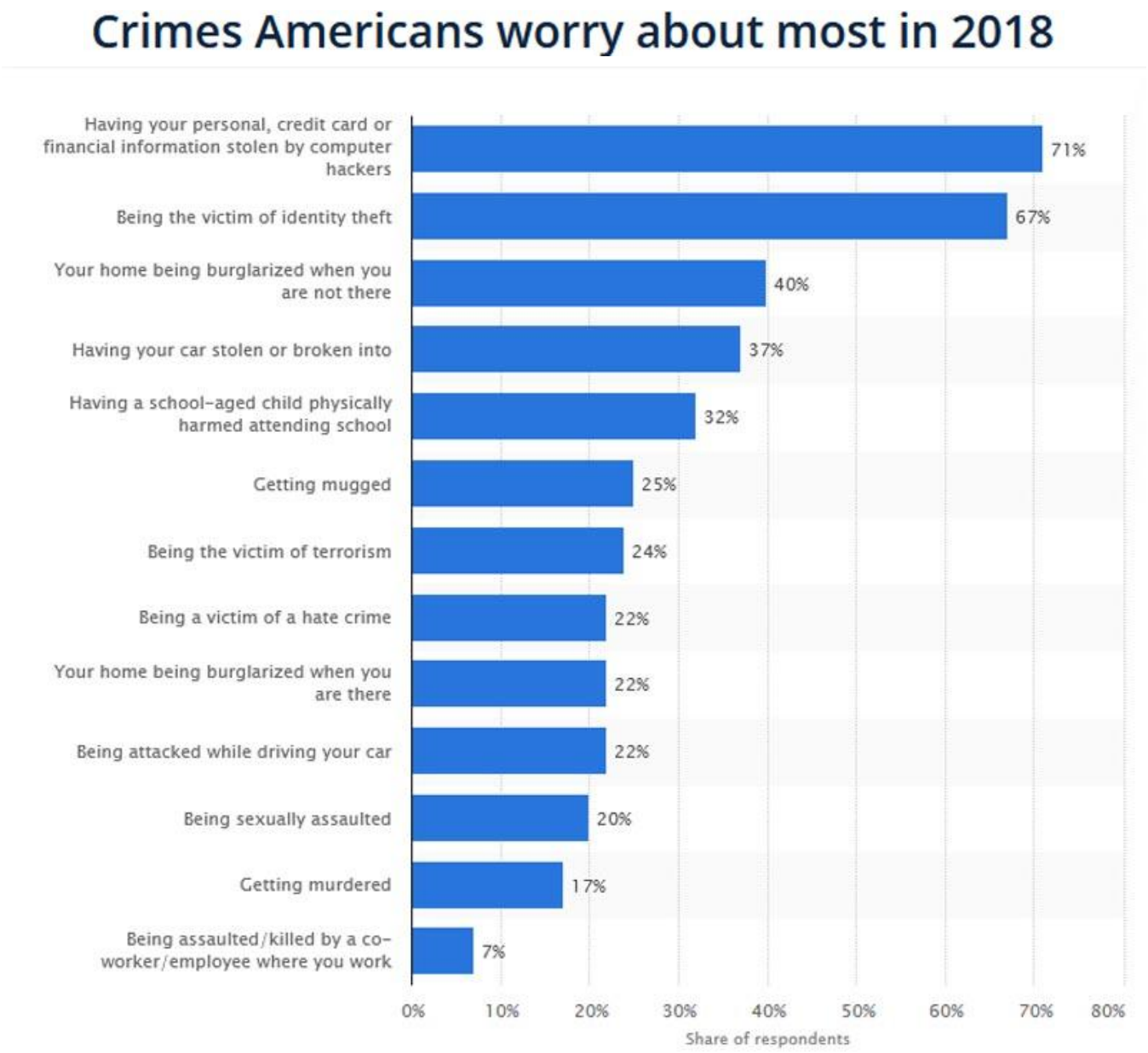
Occupation Category	Number	Percent
Information	125,811,000	80.8
Other*	29,950,00	19.2
Total	155,761,000	100.0

The data indicate that almost 81% of American employees either create (research occupations), distribute (media and Internet occupations), manipulate (various analyst occupations, among others), or otherwise use information in their jobs. Thus, a large majority of Americans depend on information in some way for their livelihood. In this context, the social costs of cybercrime include damage and destruction of data (various types of malware), lost productivity, theft of intellectual property (piracy), theft of personal (and financial) data, disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems (ransomware), and reputational harm. In brief, cybercrime costs residents of an information society not just economically (see below), but also socially in that it attacks the foundation of the social organization of work and even of leisure pursuits

* Includes categories: Manufacturing; Construction; Agriculture and related; Mining, quarrying, and oil and gas extraction

Here are some other data on cybercrime in the United States. One measure of the social consequences of cybercrime is the beliefs and perceptions people have of it. If people are aware of cybercrime or are concerned/worried about being victims of cybercrime, this is an indication that cybercrime has entered the public consciousness. Once people are cognizant of cybercrime, they are likely to take it into account (think about it) as they use their computers or other digital devices in their jobs, for their consumer purchases, for entertainment, or any other application(s). Once people feel they must adjust their computing usage to the potential pernicious effects of cybercrime, that feeling is evidence of the social effects of cybercrime.

First, what types of crime do Americans worry about most?



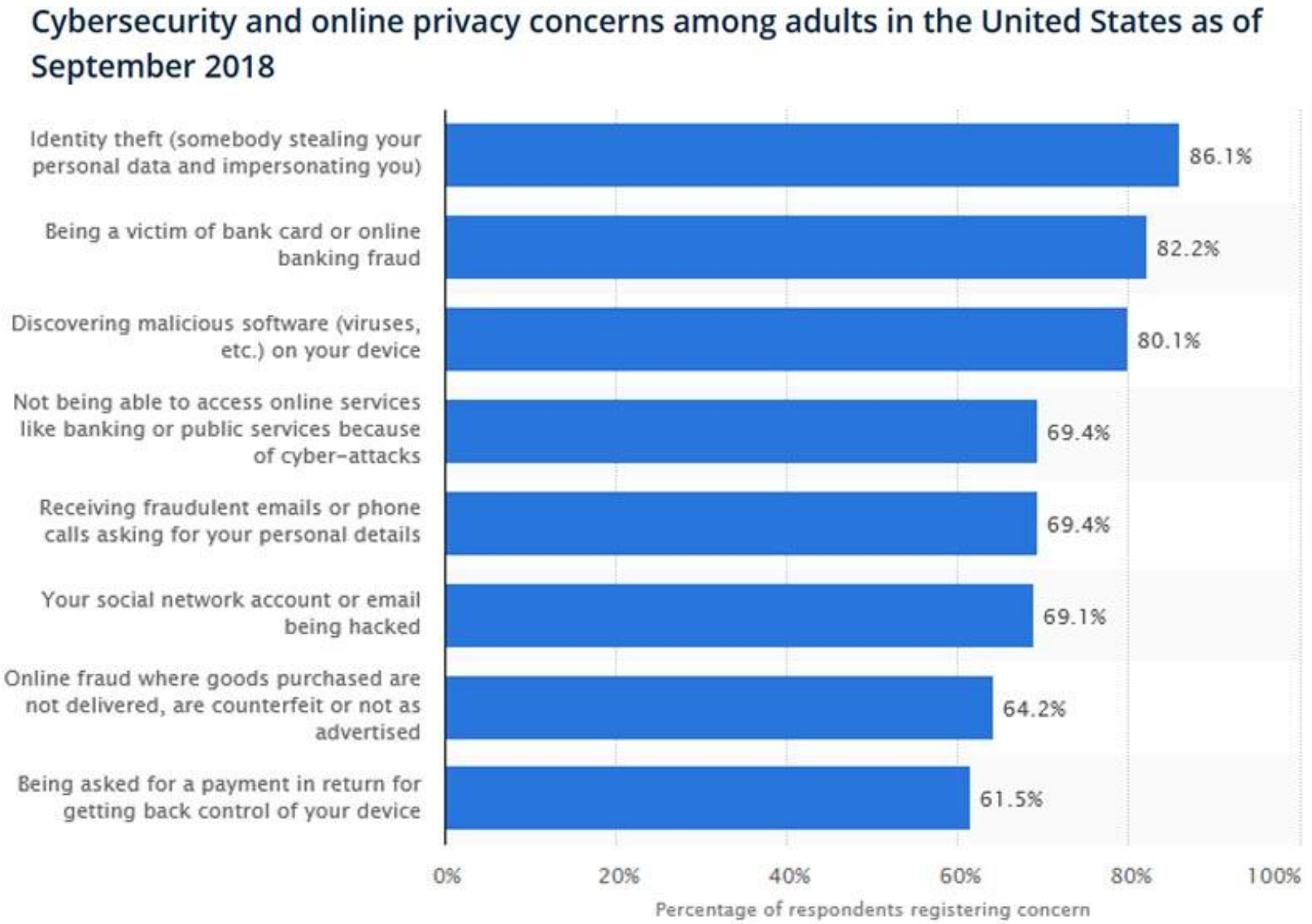
How aware are Americans of the risks they face of being victims of cybercrime?

Level of cybercrime risk awareness among adults in the United States as of September 2018, by region

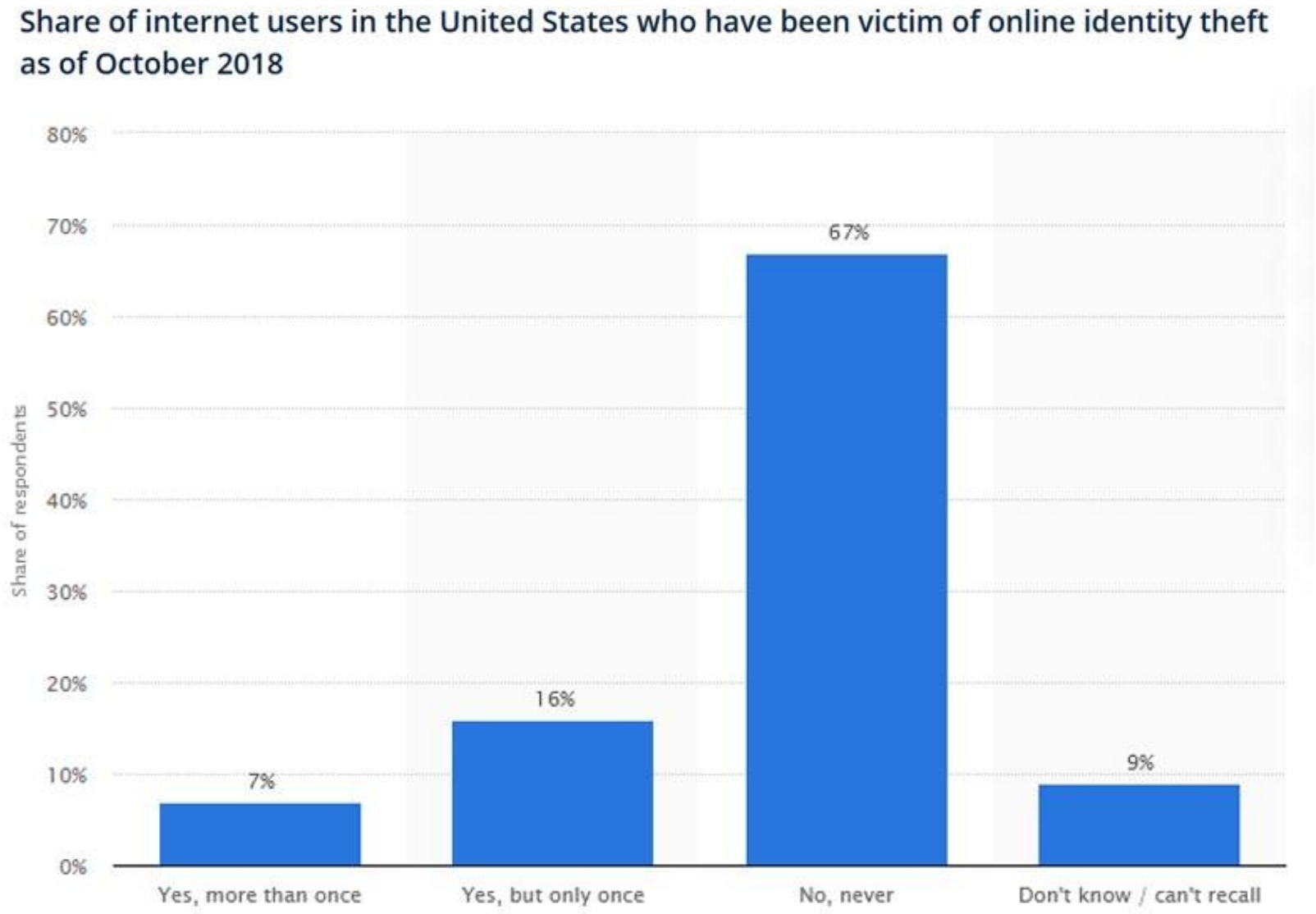
	South	West	Midwest	Northeast	US Overall
Very well informed	21.1%	19.6%	16.5%	20.5%	19.7%
Fairly well informed	49.6%	50.1%	52.4%	52.3%	50.8%
Not very well informed	22.9%	25%	26.2%	21.7%	23.9%
Not at all informed	3.4%	2.6%	2.5%	2.3%	2.6%
Don't know	3%	2.8%	2.5%	3.3%	3%

Showing entries 1 to 5 (5 entries in total)

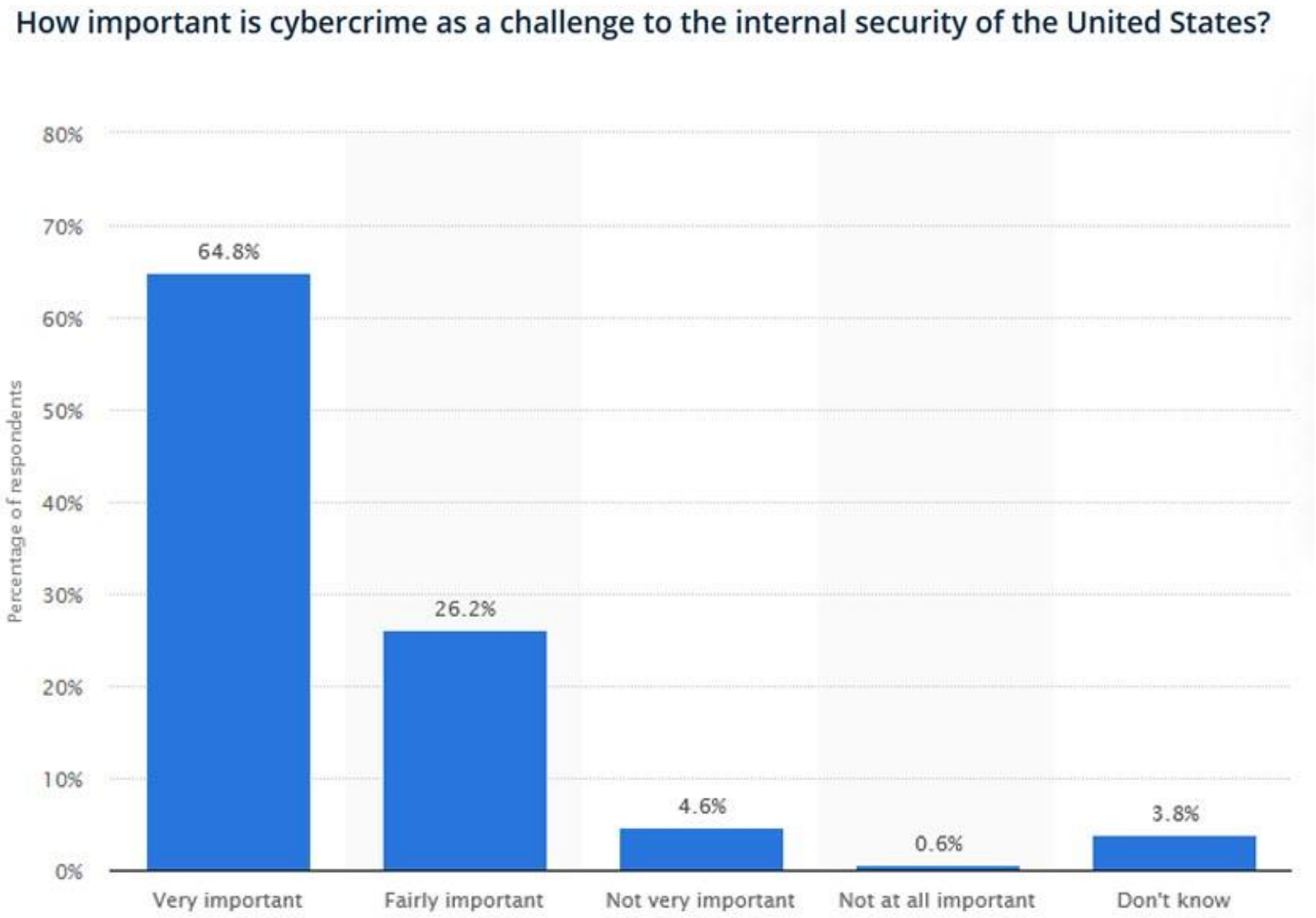
What concerns do Americans have about being victims of cybercrime?



What percentage of Americans have been victims of identity theft?



What percentage of Americans view cybercrime as a threat the security of the United States?



The economic costs of cybercrime are more readily quantifiable and are thus somewhat easier to see and understand. Many forms of cybercrime have direct economic costs: theft of financial data and money from individuals; embezzlement from organizations and businesses; various fraud schemes; ransomware. Let's start with a global picture of the costs of cybercrime.
In a report, Economic Impact of Cybercrime, the Center for Strategic and International Studies presents the table on the next slide. The numbers are estimates of each region's Gross Domestic Product (GDP) in United States dollars (USD), Cybercrime costs, and the Amount of money lost to cybercrime.

Region (World Bank)	Region GDP (USD, trillions)	Cybercrime Cost (USD, billions)	Cybercrime Loss (% GDP)
North America	20.2	140 to 175	0.69 to 0.87%
Europe and Central Asia	20.3	160 to 180	0.79 to 0.89%
East Asia & the Pacific	22.5	120 to 200	0.53 to 0.89%
South Asia	2.9	7 to 15	0.24 to 0.52%
Latin America and the Caribbean	5.3	15 to 30	0.28 to 0.57%
Sub-Saharan Africa	1.5	1 to 3	0.07 to 0.20%
MENA	3.1	2 to 5	0.06 to 0.16%
World	**$75.8**	**$445 to $608**	**0.59 to 0.80%**

Table 2. Regional Distribution of Cybercrime 2017

MENA: Middle East, North Aftica

In the Official 2019 Annual Cybercrime Report, Cybersecurity Ventures reported that cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015.

The White House Council of Economic Advisors wrote in its 2018 report:

We estimate that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016.