# THE STATISTICS OF CYBER-CRIME AMONG THE WORLD

**Safarova Noila Erkin qizi**
*The second year student of Termiz state university*
**Tursunov Behruz Normurod o'g'li**
*the teacher of Law faculty in Termiz state university*

**Annotation:** *This article will discuss about improving statistics of cyberbullying these days among the world and insured businesses against cybercrime attacks and about challenges in pricing cyber-insurance.*

**Keywords:** *cyberbullying, digital space, Cyber Security Centre, cyber-insurance, methodological limitations, financial value, lack of awareness, victim of cyberbullying.*

As the name implies, cyberbullying is bullying in a digital space, such as on mobile phones, computers, tablets, etc., in arenas such as text messaging, social media, forums, online gaming, and more.

Even in 2023, bullying is still a problem for most people. 73 percent of students feel they were bullied in their lifetime, and 44 percent say it's happened in the last 30 days. It should come as no surprise that cyberbullying has become a major issue. All that has happened is that an age-old problem has made its way into the digital world.

One could argue that cyberbullying is more damaging than traditional in-person bullying because it can happen anytime. The words people use to bully are in the digital space, so cyberbullying is more challenging to spot, meaning it often goes unnoticed.

To see how big of a problem this is, here are all the statistics about cyberbullying that you need to know:

In the past financial year, the Australian Cyber Security Centre received 76,000 cyber-crime reports – on average, one every seven minutes. The year before, it was a report every eight minutes. The year before that, every ten minutes.

The study also revealed some surprising statistics about the number of people that are perpetrators of cyberbullying. For example, they found that:

69 percent of people report having done something abusive towards others online.

15 percent of people admit to having cyberbullied someone else online.

These statistics are troubling because it suggests a general misunderstanding of precisely what cyberbullying is.

More specifically, it's likely these people who have admitted to doing something abusive towards others online actually engaged in cyberbullying. Still, because of a lack of awareness about this, they do not admit it.

Here are some more cyberbullying statistics to consider:

According to StopBullying.gov, over half of students who identify as being LGBTQ have experienced cyberbullying at some point.

Girls are more likely to be a victim of cyberbullying than boys. Overall, around 36 percent of girls have reported being cyberbullied compared to 26 percent of boys, according to a report from Pew Research Center.

While a report from Florida Atlantic University states that 83 percent of those bullied online have also been bullied in person, and 69 percent who admitted to bullying online have also admitted to in-person bullying.

The growth of cyber crime means it is now arguably the top risk facing any business with an online presence. One successful cyber-attack is all it takes to ruin an organization's reputation and bottom line. The estimated cost to the Australian economy in 2021 was $42 billion.

To protect itself (and its customers), a business has three main options. It can limit the amount of sensitive data it stores. It can take greater care to protect the data it does store. And it can insure itself against the consequences of a cyber-attack.
Cyber-insurance is a broad term for insurance policies that address losses as a result of a computer-based attack or malfunction of a firm's information technology systems. This can include costs associated with business interruptions, responding to the incident and paying relevant fines and penalties.

The global cyber-insurance market is now worth an estimated US$9 billion (A$13.9 billion). It is tipped to grow to US$22 billion by 2025.

But a big part of this growth reflects escalating premium costs – in Australia they increased more than 80% in 2021 – rather than more business taking up insurance.

So coverage rates are growing slowly, with about 75% of all businesses in Australia having no cyber-insurance, according to 2021 figures from the Insurance Council of Australia.

Challenges in pricing cyber-insurance

With cyber-insurance still in its infancy, insurers face significant complexities in quantifying cyber risk pricing premiums accordingly – high enough for the insurers not to lose money, but as competitive as possible to encourage greater uptake.

A 2018 assessment of the cyber-insurance market by the US Cybersecurity and Infrastructure Security Agency identified three major challenges: lack of data, methodological limitations, and lack of information sharing.

Lack of historical loss data means insurers are hampered in accurately predicting risks and costs.

Because of the relative newness of cyber crime, many insurers use risk-assessment methodologies derived from more established insurance markets such as for car, house and contents. These markets, however, are not analogous to cyber crime.

Companies may be hesitant to disclose information about cyber incidents, unless required to do so. Insurance carriers are reluctant to share data pertaining to damage and claims.

This makes it hard to create effective risk models that can calculate and predict the likelihood and cost of future incidents.

So what needs to be done?

Deakin University's Centre for Cyber Security Research and Innovation has been working with insurance companies to understand what must be done to improve premium and risks models pertaining to cyber insurance.

First, greater transparency is needed around cyber-related incidents and insurance to help remedy the lack of data and information sharing.

The federal government has taken two steps in the right direction on this.

One is the Consumer Data Right, which provides guidelines on how service providers must share data about customers. This came into effect in mid-2021.

The other is the government's proposal to amend privacy legislation to increase penalties for breaches and give the Privacy Commissioner new powers.

Second, insurers must find better ways to measure the financial value and worth of the data that organisations hold.

The primary asset covered by cyber insurance is the data itself. But there is no concrete measure of how that data is worth.

The recent Optus and Medibank Private data breaches provide clear examples. The Optus event affected millions more people than the Medibank Private hack, but the Medibank Private data includes sensitive medical data that, in principle, is worth far more than data regarding just your personal identity.

Without an accurate way to measure the financial value of data, it is difficult to determine the appropriate premium costs and coverage.

Cyber insurance is a new, specialized market with significant uncertainty. Given the ever-increasing risks to individuals, organizations and society, it is imperative that insurers develop robust and reliable risk-based models as soon as possible.

This will require a consolidated effort between cyber-security experts, accountants and actuaries, insurance professionals and policymakers.

## REFERENCES:

1. https://www.broadbandsearch.net/blog/cyber-bullying-statistics
2. Florida Atlantic University states reports.
3. https://cyberbullying.org/new-national-bullying-cyberbullying-data.
4. Australian Cyber Security Centre reports.