RISING FREQUENCY AND COST OF CYBERCRIME IN K-12

CENTRIPETAL

RISING FREQUENCY AND COST OF CYBERCRIME IN K-12

The education sector is a goldmine for cyber criminals. The combination of high-risk behaviors, limited security budgets, and sensitive personal information that can be monetized in various ways, is driving up both the cost and frequency of breaches.

Several factors may contribute to the increase, including:

Increased Digitization:

With the growing use of technology in education, there's a greater reliance on digital systems to store and manage student records, making them more vulnerable to cyberattacks.

Lack of Cybersecurity Measures:

Many educational institutions, especially those with limited budgets, may not have robust cybersecurity measures in place to protect against sophisticated cyber threats.

Human Error:

Data breaches can also occur due to human error, such as employees falling victim to phishing scams or unintentionally exposing sensitive information.

Target for Cybercriminals:

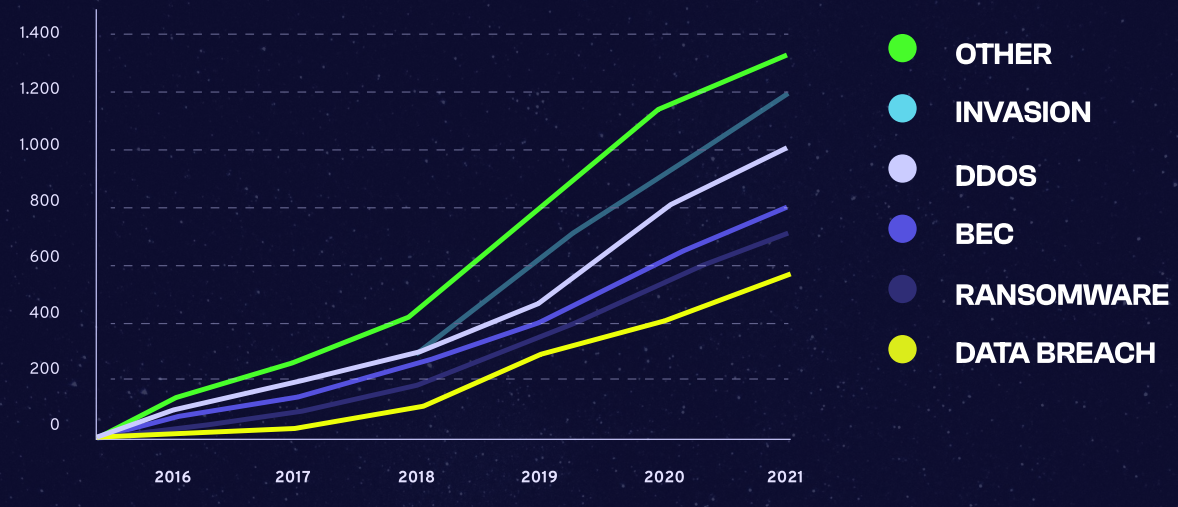
K-12 institutions may be seen as easier targets compared to larger organizations, making them more susceptible to attacks.

Ransomware Attacks:

Ransomware attacks, where hackers encrypt data and demand payment for its release, have become increasingly common in various sectors, including education.

The K-12 Security Information Exchange, an organization focused on addressing cybersecurity challenges in K-12 educational institutions, shared that there were over 1,600 publicly-disclosed incidents between 2016-2022. However, anecdotal evidence suggests 10-20 times more K-12 cyber incidents go undisclosed every year.

NUMBER OF PUBLICLY-DISCLOSED K-12 CYBER INCIDENTS BY INCIDENT TYPE: 2016-2021



THE COST OF CYBERCRIME IS ON THE RISE

Today, school districts are struggling under the burden of more damaging cyber attacks than ever before and costs of recovery from such attacks can be staggering.

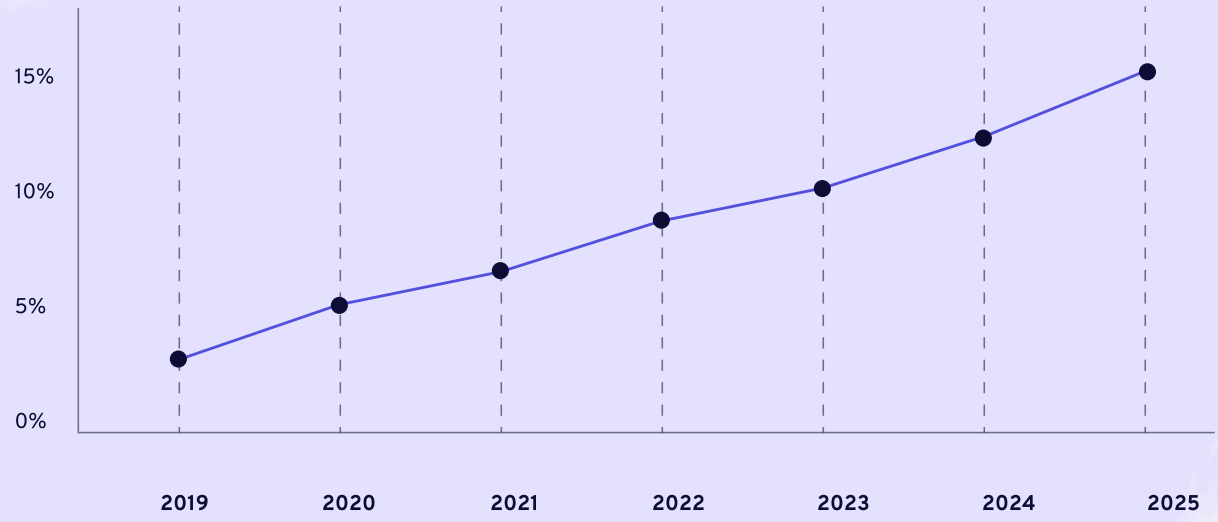
$8 trillion

The global cost of cybercrime

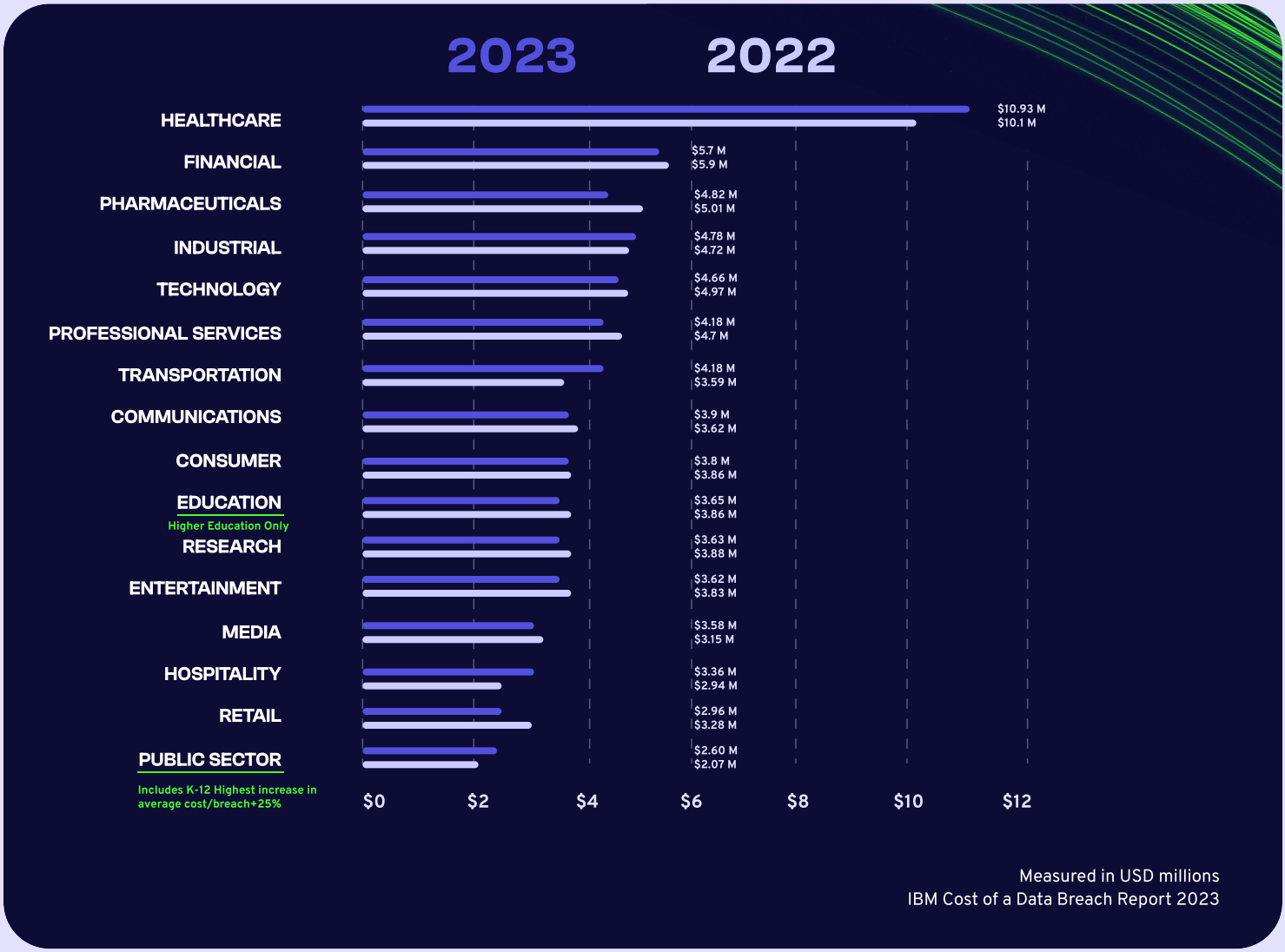
$10.5 trillion

estimated to hit by 2025

CYBERSECURITY VENTURES: 2022 OFFICIAL CYBERCRIME REPORT



In IBM's Cost of a Data Breach Report 2023, they've looked at 500 breaches broken down by vertical and geography.



While the healthcare industry is the most expensive in terms of breaches, the public sector, which includes K-12, is the fastest growing.

The public sector cost per breach was reported to be at $2.6 million dollars in 2023, which represents a 25% growth from $2.07 million in 2022.

To combat the rising cost and the number of breaches, it's crucial for educational institutions to prioritize cybersecurity measures and pivot a once reactive mindset to proactive defense. As a result, their security teams will be more efficient and effective, without incurring substantial cost or expanding their cyber analyst teams.

For More Information

centripetal.ai


CENTRIPETAL
centripetal.ai