Cybersecurity Ventures Estimates Global Cybercrime Costs Will Be $6 Trillion In 2021

If it were measured as a country, then cybercrime would be the world's third-largest economy after the U.S. and China.

SAUSALITO, CA, USA, December 7, 2020 /EINPresswire.com/ -- Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $6 trillion in 2021 and $3 trillion in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined.

> If it were measured as a country, then cybercrime would be the world's third-largest economy after the U.S. and China."
>
> *Steve Morgan, Editor-in-Chief at Cybercrime Magazine*

The damage cost estimation is based on historical cybercrime figures including recent year-over-year growth, a dramatic increase in hostile nation-state sponsored and organized crime gang hacking activities, and a cyberattack surface which will be an order of magnitude greater in 2025 than it is today.

Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.

Organized cybercrime entities are joining forces, and their likelihood of detection and prosecution is estimated to be as low as 0.05 percent in the U.S., according to the World Economic Forum's 2020 Global Risk Report.

CYBERSECURITY SPENDING

In 2004, the global cybersecurity market was worth $3.5 billion — and in 2017 it was worth more than $120 billion. The cybersecurity market grew by roughly 35X during that 13-year period —

prior to the latest market sizing by Cybersecurity Ventures.

Global spending on cybersecurity products and services for defending against cybercrime is projected to exceed $1 trillion cumulatively over the five-year period from 2017 to 2021.

“Most cybersecurity budgets at U.S. organizations are increasing linearly or flat, but the cyberattacks are growing exponentially,” says Mark Montgomery, Executive Director at the U.S. Cyberspace Solarium Commission (CSC), which was established develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences.

The FY 2020 U.S. President’s Budget includes $17.4 billion of budget authority for cybersecurity-related activities, a $790 million (5 percent) increase above the FY 2019 estimate, according to The White House. Due to the sensitive nature of some activities, this amount does not represent the entire cyber budget.

Cybersecurity Ventures anticipates 12-15 percent year-over-year cybersecurity market growth through 2025. While that may be a respectable increase, it pales in comparison to the cybercrime costs incurred.

CYBERWARFARE IN THE C-SUITE

A new report from Cybersecurity Ventures, sponsored by INTRUSION, Inc., focuses boardroom executives on the costs and consequences of cybercrime.

CSC has an urgent message for boardroom and C-suite executives: The status quo in cyberspace is unacceptable, which is spelled out in its groundbreaking 2020 Report which proposes a strategy of layered cyber deterrence — to protect all U.S. businesses and governments from cybercrime and cyberwarfare. But, this is hardly the first warning. “Some of the same things we’re recommending today, we were pushing 23 years ago,” says Montgomery.

“Every company should have a CISO or cybersecurity expert on their board — because cybercrime is the greatest risk to business continuity that every company faces,” says Jack B. Blount, President & CEO at INTRUSION, Inc. The idea is to put someone in the boardroom who will wave the red flag and get everyone else paying attention to the severity of the risk. Montgomery agrees and says attention is the number one priority, not bringing in a new CISO — instead empower the CISO that you have.

The value of a business depends largely on how well it guards its data, the strength of its cybersecurity, and its level of cyber resilience.

The full report can be seen at https://OfficialCybercrime.com

Editor-In-Chief
Cybersecurity Ventures
+1 631-680-8660
email us here
Visit us on social media:
Twitter
LinkedIn
