Cybersecurity Market: 35X Growth Past 13 Years; $1 Trillion Next 5 Years

Cybercrime damage costs will reach $6 trillion annually by 2021, continues to fuel cybersecurity market growth

MENLO PARK, CA, UNITED STATES, February 20, 2017 /EINPresswire.com/ -- CYBERSECURITY MARKET REPORT, Q1 2017

Cybersecurity Ventures predicts global spending on cybersecurity products and services will exceed $1 trillion cumulatively over the next five years, from 2017 to 2021.

> We anticipate 12-15 percent year-over-year cybersecurity market growth through 2021"
> *Steve Morgan, Cybersecurity Ventures*

In 2004, the global cybersecurity market was worth $3.5 billion — and in 2017 we expect it to be worth more than $120 billion. The cybersecurity market grew by roughly 35X over 13 years.

While all other tech sectors are driven by reducing inefficiencies and increasing productivity, cybersecurity spending is driven by cybercrime. The unprecedented cybercriminal activity we are witnessing is generating so much cyber spending, it's become nearly impossible for analysts to accurately track.

We anticipate 12-15 percent year-over-year cybersecurity market growth through 2021, compared to the 8-10 percent projected over the next five years by several industry analysts.

IT analyst forecasts are unable to keep pace with the dramatic rise in cybercrime, the ransomware epidemic, the refocusing of malware from PCs and laptops to smartphones and mobile devices, the deployment of billions of under-protected Internet of Things (IoT) devices, the legions of hackers-for-hire, and the more sophisticated cyber-attacks launching at businesses, governments, educational institutions, and consumers globally.

It is likely that analyst firms will catch up with our projections in 2017 — and update the disproportionately low share of total IT spending which security is expected to account for (over the next 5 years) in their current reports. By 2020, we expect IT analysts covering cybersecurity will be predicting five-year spending forecasts (to 2025) at well over $1 trillion.

IT SECURITY SPENDING HAS BECOME MORE DIFFICULT TO TRACK

Historic analyst reports are rooted in 'IT security' (servers, networking gear, data centers and IT infrastructure, PCs, laptops, tablets, and smartphones) and not fully evolved to 'cybersecurity' which includes non-computer devices and non-IT centric platforms and environments — which covers entire

sub-markets i.e. aviation security, automotive security, IoT security, and IIoT (Industrial Internet of Things) security. All of those market segments combined make up the cybersecurity market.

Even IT security services are difficult to fully size. Tech is a cottage industry which includes tens of thousands of VARs (value-added-resellers), IT solution providers, and SIs (systems integrators) who wrap IT security services around the IT infrastructures they implement and support — but (most of) these firms don't break out and report cybersecurity revenues as a separate bucket.

"A large portion of information security related spending is not accounted for as being information-security related" writes Joseph Steinberg, an Inc. Magazine columnist covering cybersecurity. "Consider, for example, that an organization developing a software package for internal use might spend money from its development budget on technology to scan code for vulnerabilities – the expenditure, however, may never be tracked back to an information-security budget" adds Steinberg.

Big branded tech companies with sizable professional services organizations providing cybersecurity services have yet to set up specific divisions or revenue reporting which analysts need in order to capture accurate market figures.

There's also many new players getting into cybersecurity. CPAs and attorneys who used to answer their clients' what-if and what-now questions around data breaches — are now starting up lucrative cyber consulting divisions.

The IT Security Spending Survey — published by SANS Institute in 2016 — states "Tracking security-related budget and cost line items to justify expenditures or document trends can be difficult because security activities cut across many business areas, including human resources, training and help desk.

SANS states that most organizations fold their security budgets and spending into another cost center, whether IT (48%), general operations (19%) or compliance (4%), where security budget and cost line items are combined with other related factors. Only 23% track security budgets and costs as its own cost center. SANS makes an astute observation which may account for the shortfall in IT spending projections by some researchers and analysts.

CONSUMER CYBERSECURITY SPENDING IS NOT FULLY ACCOUNTED FOR

Consumer spending on information-security is often impossible to track, according to an Inc. Magazine article. How can analysts possibly know, for example, when, after a malware infection, someone pays a consultant to wipe and restore-to-factory-settings his or her computer or smartphone.

Spending in the consumer category includes personal identity theft protection services, computer and mobile phone repair services specific to malware and virus removal, installation of anti-virus and malware protection software, post-breach services including data recovery and user education on best practices for personal cyber defense.

The consumer cybersecurity market is much bigger than just the anti-virus and malware defense apps that are purchased or come pre-installed. Much like corporations, consumers are spending time and money as a result of cyber-attacks.

CYBERCRIME FUELS MARKET GROWTH

Cybercrime damages will cost the world $6 trillion annually by 2021

Cybersecurity Ventures predicts cybercrime will continue rising and cost businesses globally more than $6 trillion annually by 2021. The estimate 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, a cyber attack surface which will be an order of magnitude greater than it is today, and the cyber defenses expected to be pitted against hackers and cybercriminals over that time.

The cybercrime cost prediction includes 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.

The worldwide cyber damage estimates do not include unreported cybercrimes, legal and public relations fees, declines in stock and public company valuations directly and indirectly related to security breaches, negative impact on post-hack ability to raise capital for start-ups, interruptions to e-commerce and other digital business transactions, loss of competitive advantage, departure of staff and recruiting replacement employees in connection with cyber-attacks and resulting losses, ongoing investigations to trace stolen data and money, and other.

Stay tuned for the Cybersecurity Market Report, Q2 2017 edition.

– Steve Morgan is founder and Editor-In-Chief at Cybersecurity Ventures

Editor-In-Chief
Cybersecurity Ventures
631-680-8660
email us here
