McAfee
Together is power.

The Economic Impact of Cybercrime—No Slowing Down

Cybercrime now costs the world almost $600 billion, or 0.8 percent of global GDP, according to a new report by the Center for Strategic and International Studies (CSIS) and McAfee. Scheduled for release February 21, "The Economic Impact of Cybercrime: No Slowing Down" updates the popular 2014 report, which put global losses at close to $500 billion, or 0.7% of global income.

When you look at the cost of cybercrime in relation to the worldwide internet economy—$4.2 trillion in 2016—cybercrime can be viewed as a 14% tax on growth[1].

To put the latest statistic in perspective, it amounts to more than the income of almost all but a few countries. When you look at the cost of cybercrime in relation to the worldwide internet economy—$4.2 trillion in 2016—cybercrime can be viewed as a 14% tax on growth[1].

As crimes with global impact go, cybercrime ranks third, behind government corruption and narcotics as a global economic scourge[2], and here's why:

- **It touches everyone:** Nearly two-thirds of people who use online services (more than two billion individuals)—have had their personal data stolen or compromised.
- **Low-risk to high payoff:** The probability of getting arrested or going to jail is low. Not one of the perpetrators of the biggest headline-grabbing breaches has been prosecuted. Law enforcement agencies are stepping up their efforts, but many cybercriminals operate outside of their jurisdictions.

The report attributes the $100 billion growth in cybercrime to cybercriminals quickly adopting new technologies, the ease of engaging in cybercrime—including an expanding number of cybercrime centers—and the growing financial sophistication of top-tier cybercriminals.

Connect With Us

Key Findings

- Ransomware is the fastest growing cybercrime tool, with more than 6,000 online criminal marketplaces selling ransomware products and services, and ransomware-as-a-service gaining in popularity.
- Cybercrime-as-a-service in general has become more sophisticated with flourishing markets offering a broad array of tools and services such as exploit kits, custom malware and botnet rentals.
- The threat of law enforcement action has forced most cybercrime dealings onto the dark web, where the anonymity of cryptocurrencies (e.g., Tor and Bitcoin) protects actors from easy identification.
- Popular malware on the dark web includes web injections, exploit kits and infrastructure-as-a-service, such as bulletproof hosting and botnet rentals.
- The theft of intellectual property accounts for at least a quarter of the cost of cybercrime and, when it involves military technology, creates risks to national security as well.

Elements of Cyber Crime

The report did not attempt to measure the cost of all malicious activity on the internet, focusing instead on criminals gaining illicit access to a victim's computer or network. The elements of cybercrime the authors identify include:

- The loss of IP and business-confidential information
- Online fraud and financial crimes, often the result of stolen personally identifiable information
- Financial manipulation directed toward publicly-traded companies
- Opportunity costs, including disruption in production or services and reduced trust in online activities
- The cost of securing networks, purchasing cyber insurance and paying for recovery from cyber-attacks
- Reputational damage and liability risk for the affected company and its brand

Fastest Growing Threat

Ransomware targets everyone—from large enterprises to consumers. While not every victim pays the ransom, there are plenty who do.

According to the FBI, $209 million in ransom was paid in the first quarter of 2016, compared to $24 million in all of 2015.[3] Here's why ransomware has seen such explosive growth[4]:

- The availability of ransomware kits in the web underground, with more than 6,000 online criminal marketplaces offering a total of 45,000 different products and services
- Ransomware-as-a-Service (RaaS) platforms that provide ransomware authors with an opportunity to extend their reach by sharing their code for a fee with the criminal community and taking a cut of the collected ransoms
- Ransomware worms, like WannaCry, that can spread throughout the network and lock up multiple computers

As crimes with global impact go, cybercrime ranks third, behind government corruption and narcotics as a global economic scourge.[2]

Other trends that we expect to see for ransomware are data exfiltration capabilities and attacks on mobile and Internet of Things (IoT) devices, which typically lack strong defenses.

Cybercrime Around the World

The report measures cybercrime in North America, Europe and Central Asia, East Asia & the Pacific, South Asia, Latin America and the Caribbean, Sub-Saharan Africa and MENA. The report's findings suggest that the cost of cybercrime across regions varies, depending on each country's level of cybersecurity maturity, which is measured according to these key indicators: legal measures, technical measures, organizational measures, capacity building, and cooperation.

The results were categorized as follows: top-tier countries with digital economies and mature cybersecurity, mid-tier countries that are evolving their digitized economy and cybersecurity, and countries whose digital economies and cybersecurity efforts are at the beginning stages. As you might expect, wealthier nation-states suffer higher cybercrime losses. Those hit hardest are in the mid-tier.

- **Brazil:** It is the second leading source of cyberattacks and the third most-affected target.
- **Germany:** The country is home to the most sophisticated underground internet economy in the EU.
- **Japan:** Previously protected from cybercrime because of the language barrier and no infrastructure for money laundering, Japan is seeing an increase, especially in attacks targeting banks.
- **United Kingdom:** Online fraud and cybercrime account for nearly half of all crimes, amounting to more than 5.5 million offenses annually.
- **United Arab Emirates:** It is the second most targeted country in the world, with the cost of cybercrime estimated at $1.4 billion per year.

Conclusion and Recommendations

While the analysis provided by CIS and McAfee focuses on the costs of cybercrime, there are several steps that both organizations and nation-states can take as a way to reduce losses:

- Consistent implementation of key security measures, such as regular security software update and patching and open security architectures, along with investment in advanced defenses that span everything from endpoint devices to the cloud
- Increased international law enforcement cooperation among nations and the private sector and investment in more resources for investigation—especially among developing nations
- Modernization of current processes, such as the Mutual Legal Assistance Treaty (MLAT), which allows governments to enlist the help of other government in cybercrime investigations and evidence collection
- Better collection of aggregate data by national authorities
- Standardization of threat information and coordination of cybersecurity requirements to boost security in critical sectors like finance

The report attributes the $100 billion growth in cybercrime to cybercriminals quickly adopting new technologies, the ease of engaging in cybercrime—including an expanding number of cybercrime centers—and the growing financial sophistication of top-tier cybercriminals.

- Accelerated adoption of treaties like the Budapest Convention, which defines the responsibilities of nation-states for cybercrime law enforcement and cooperation
- Imposition of temporary penalties or other consequences on governments that fail to take action against cybercrime

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place.
www.mcafee.com

1. https://www.bcg.com/documents/file100409.pdf
2. www.imf.org/external/pubs/ft/sdn/2016/sdn1605.pdf
3. Max Metzger. "FBI says Ransomware soon becoming a billion dollar business." SC Media UK, January 10, 2017. https://www.scmagazineuk.com/fbi-says-ransomware-soon-becoming-a-billion-dollar-business/article/630615/
4. "McAfee Labs Threat Report," McAfee, December 2017

McAfee
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com