McAfee
An Intel Company

Report Summary

Net Losses: Estimating the Global Cost of Cybercrime

Economic impact of cybercrime II

Executive Summary

Cybercrime is a growth industry. The returns are great, and the risks are low. We estimate that the likely annual cost to the global economy from cybercrime is more than $445 billion, including both the gains to criminals and the costs to companies for recovery and defense. A conservative estimate would be $375 billion in losses, while the maximum could be as much as $575 billion. This is more than the national income of most countries and is equivalent to between 0.5% and 0.8% of global income.

Putting a number on the cost of cybercrime and cyberespionage is the headline, but the dollar figure begs important questions about the damage to the victims from the cumulative effect of losses in cyberspace. Cybercrime includes the effect of hundreds of millions of people having their personal information stolen. One estimate puts the total at more than 800 million individual records in 2013. This alone could cost as much as $160 billion per year. The constant reports of companies being hacked contribute to a growing sense that cybercrime is out of control.

The most important cost of cybercrime, however, comes from the damage it does to company performance and to national economies. Our estimate used data that takes into account the loss of intellectual property, the theft of financial assets and sensitive business information, opportunity costs, additional costs for securing networks, and the cost of recovering from cyberattacks, including reputational damage to the hacked company. Our sources include published data, interviews, and estimates by government agencies and companies around the world.

We found hundreds of reports of companies being hacked. The US, for example, notified 3,000 companies in 2013 that they had been hacked. Two banks in the Persian Gulf lost $45 million. A British company reported that it lost $1.3 billion. Brazilian banks say customers lose millions annually. India's CERT reported that 308,371 websites were hacked between 2011 and June 2013. Simply adding up the losses from the known incidents would total billions of dollars, and there are too many anecdotes to list. Given the number of incidents, it is surprising that many countries make little or no effort to produce official estimates of cybercrime losses. This is true even for large and developed countries. And it is especially true of middle- and lower-income countries. This failure obviously affects all efforts to estimate losses with precision.

G20 nations suffer the bulk of losses. Losses from cybercrime for four largest economies in the world (the US, China, Japan, and Germany) reached $200 billion. Low-income countries have smaller losses, but this will change as these countries increase their use of the Internet and as cybercriminals move to exploit mobile platforms. For developed countries, cybercrime has serious implications for employment. The effect is to shift employment away from jobs that create the most value. Our first report showed that losses from cybercrime could translate into more than 200,000 jobs lost in the US. Using European Union data, we estimate that Europe could lose as many as 150,000 jobs from cybercrime. While translating cybercrime losses directly into job losses is not easy, the effect on employment cannot be ignored.

G20 nations suffer the bulk of losses and losses from cybercrime for four largest economies in the world (the US, China, Japan, and Germany) reached $200 million. Low-income countries have smaller losses, but this will change as these countries increase their use of the Internet and as cybercriminals move to exploit mobile platforms.

IP Theft and Innovation Cannibalism

Intellectual property (IP) losses are the most difficult to estimate for the cost of cybercrime, but it is also is the most important variable for determining loss. IP theft shifts trade balances and national employment. Countries where IP creation and IP-intensive industries are important for wealth creation lose more in trade, jobs, and income from cybercrime. The effect of cyberespionage on national security is significant, and the monetary value of the military technology taken does not reflect the full cost to victim countries. Cybercrime damages innovation. One way to think about the cost from cybercrime is to ask how investors would act if returns on innovation doubled. Companies would invest more and the global rate of innovation would increase. By eroding the returns on intellectual property (IP), cybercrime invisibly creates a disincentive to innovation.

Risk-Free Financial Crime

When millions of people have their credit card information stolen by hackers, it gets immediate attention. Financial crime usually involves fraud, but this can take many forms to exploit consumers, banks, and government agencies. The most damaging financial crimes penetrate bank networks, with cybercriminals gaining access to accounts and siphoning out money. High profile cyberheists that steal tens of millions of dollars from banks are a global phenomenon.

Retailers are a favorite target for cybercriminals. In 2013, a series of high-loss attacks added to a list that includes TJ Maxx, Sony, and others. UK retailers reportedly lost more than $850 million in 2013. Large-scale attacks have occurred against retailers, hotel chains, an airline, and financial service companies in Australia, with losses averaging over $100 million per company. Stolen personally identifiable information (PII) and credit card data are hard to monetize, but cybercriminals are getting better at this. Since there is little risk of punishment for the hackers, this kind of cybercrime will increase.

Confidential Business Information and Market Manipulation

Stealing business confidential information—investment information, exploration data, and sensitive commercial negotiation data—can yield immediate gain. The damage to individual companies runs into the millions of dollars. One UK company told British officials that it incurred revenue losses of $1.3 billion through the loss of intellectual property loss and subsequently suffered a disadvantage in its commercial activities. Hacking of central banks or finance ministries could provide valuable economic information on the direction of markets or interest rates.

Stock market manipulation is a growth area for cybercrime. By breaking into a company's networks or into the networks of its lawyers or accountants, cybercriminals can acquire inside information on acquisition and merger plans, quarterly revenue reports, or other data that affects a company's stock prices. Criminals taking advantage of this information for trading could be hard to detect. Turkey's financial regulators, for example, found suspicious activity intended to manipulate markets and stock prices that went beyond "pump and dump" schemes. For high-end cybercriminals, their primary activities may be evolving into financial manipulation that will be exceptionally difficult to detect.

Opportunity Cost

Opportunity cost is the value of forgone activities. Three kinds of opportunity costs determine the losses from cybercrime: reduced investment in research and development (R&D), risk-averse behavior by businesses and consumers, and increased spending on network defenses. For companies, the largest opportunity cost may be in the money spent to secure their networks. While companies would always spend on security even if risk in the digital environment was greatly reduced, there is a "risk premium" that they pay because of unstoppable cybercrime.

Another way to look at the opportunity cost of cybercrime is to see loss as a share of the Internet economy. Studies estimate that the Internet economy annually generates between $2 trillion and $3 trillion, a share of the global economy that is expected to grow rapidly. Our estimates suggest that cybercrime is equal to between 15% and 20% of the value created by the Internet, a heavy tax on the potential for economic growth and job creation.

Recovery Costs

Cleaning up cybercrime is expensive. The cost to individual companies of recovery from cyberfraud or data breaches is increasing. While criminals will not be able to monetize all the information they steal, the victim has to spend as if they could use all the stolen data. The aggregate cost for recovery is greater than the gain to cybercriminals. One study of the cost of cybercrime for Italy found that while the actual losses were only $875 million, the recovery and opportunity costs reached $8.5 billion. The bill for recovery costs is where the real damage to society begins, and the effect on a business can include damage to brand and other reputational losses and harm to customer relations and retention.

Incentives and Continued Growth

The incentives in cybercrime are classic. Cybercrime produces high returns at low risk and (relatively) low cost for the hackers. The opposite is true for defenders. Companies and individuals make decisions on how to manage the potential for loss from cybercrime by deciding how much risk they are willing to accept and how much they are willing to spend to reduce that risk. The problem with this is that if companies are unaware of their losses or underestimate their vulnerability, they will underestimate risk.

As more business activities move online, as consumers around the world connect to the Internet, and as autonomous devices are connected in the emerging Internet of things, the opportunities for cybercrime will grow. Losses from the theft of intellectual property will increase as acquiring countries improve their ability to make use of stolen IP to manufacture competing goods. Cybercrime is a tax on innovation, and slows the pace of global innovation by reducing the rate of return to innovators and investors. Governments need to begin serious, systematic effort to collect and publish data on cybercrime, to help countries and companies make better choices about risk and policy. Absent any change, what cybercrime holds for the world is increased losses and slower growth.

About McAfee

McAfee, part of Intel Security and a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), empowers businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence network, McAfee is relentlessly focused on keeping its customers safe. http://www.mcafee.com

About CSIS

For 50 years, the Center for Strategic and International Studies (CSIS) has developed practical solutions to the world's greatest challenges. As we celebrate this milestone, CSIS scholars continue to provide strategic insights and bipartisan policy solutions to help decision makers chart a course toward a better world.

CSIS is a bipartisan, nonprofit organization headquartered in Washington, DC. The Center's 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look to the future and anticipate change. http://csis.org/

McAfee
An Intel Company

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

61080rps_csis-econ-cybercrime-sum_fnl_0514