Surveillance

Does Cybercrime Really Cost $1 Trillion?

National Security Agency Director Gen. Keith Alexander speaks about cybersecurity and the new threats posed to the U.S. economy and military at the American Enterprise Institute in Washington, D.C., on July 9, 2012. (Chip Somodevilla/Getty Images)

by Peter Maass and Megha Rajagopalan
ProPublica, Aug. 1, 2012, 11:12 a.m.

Gen. Keith Alexander is the director of the National Security Agency and oversees U.S. Cyber Command, which means he leads the government's effort to protect America from cyberattacks. Due to the secretive nature of his job, he maintains a relatively low profile, so when he does speak, people listen closely. On July 9, Alexander addressed a crowded room at the American Enterprise Institute in Washington, D.C., and though he started with a few jokes — his mother said he had a face for radio, behind every general is a stunned father-in-law — he soon got down to business.

Alexander warned that cyberattacks are causing "the greatest transfer of wealth in history," and he cited statistics from, among other sources, Symantec Corp. and McAfee Inc., which both sell software to protect computers from hackers. Crediting Symantec, he said the theft of intellectual property costs American companies $250 billion a year. He also mentioned a McAfee estimate that the global cost of cybercrime is $1 trillion. "That's our future disappearing in front of us," he said, urging Congress to enact legislation to improve America's cyberdefenses.

These estimates have been cited on many occasions by government officials, who portray them as evidence of the threat against America. They are hardly the only cyberstatistics used by officials, but they are recurring ones that get a lot of attention. In his first major cybersecurity speech in 2009, President Obama prominently referred to McAfee's $1 trillion estimate. Sen. Joseph Lieberman, I-Conn., and Sen. Susan Collins, R-Maine, the main sponsors of the Cybersecurity Act of 2012 that is expected to be voted on this week, have also mentioned $1 trillion in cybercrime costs. Last week, arguing on the Senate floor in favor of putting their bill up for a vote, they both referenced the $250 billion estimate and repeated Alexander's warning about the greatest transfer of wealth in history.

A handful of media stories, blog posts and academic studies have previously expressed skepticism about these attention-getting estimates, but this has not stopped an array of government officials and politicians from continuing to publicly cite them as authoritative. Now, an examination of their origins by ProPublica has found new grounds to question the data and methods used to generate these numbers, which McAfee and Symantec say they stand behind.

One of the figures Alexander attributed to Symantec — the $250 billion in annual losses from intellectual property theft — was indeed mentioned in a Symantec report, but it is not a Symantec number and its source remains a mystery.

McAfee's trillion-dollar estimate is questioned even by the three independent researchers from Purdue University whom McAfee credits with analyzing the raw data from which the estimate was derived. "I was really kind of appalled when the number came out in news reports, the trillion dollars, because that was just way, way large," said Eugene Spafford, a computer science professor at Purdue.

Spafford was a key contributor to McAfee's 2009 report, "Unsecured Economies: Protecting Vital Information" (PDF). The trillion-dollar estimate was first published in a news release that McAfee issued to announce the report; the number does not appear in the report itself.

A McAfee spokesman told ProPublica the estimate was an extrapolation by the company, based on data from the report. McAfee executives have mentioned the trillion-dollar figure on a number of occasions, and in 2011 McAfee published it once more in a new report, "Underground Economies: Intellectual Capital and Sensitive Corporate Data Now the Latest Cybercrime Currency" (PDF).

In addition to the three Purdue researchers who were the report's key contributors, 17 other researchers and experts were listed as contributors to the original 2009 report, though at least some of them were only interviewed by the Purdue researchers. Among them was Ross Anderson, a security engineering professor at University of Cambridge, who told ProPublica that he did not know about the $1 trillion estimate before it was announced. "I would have objected at the time had I known about it," he said. "The intellectual quality of this ($1 trillion number) is below abysmal."

The use of these estimates comes amid increased debate about cyberattacks; warnings of a digital Pearl Harbor are becoming almost routine. "A cyberattack could stop our society in its tracks," Gen. Martin Dempsey, chairman of the Joint Chiefs of Staff, said earlier this year. Bloomberg reported just last week that a group of Chinese hackers, whom U.S. intelligence agencies referred to as "Byzantine Candor," have stolen sensitive or classified information from 20 organizations, including Halliburton Inc., and a prominent Washington law firm, Wiley Rein LLP.

There is little doubt that a lot of cybercrime, cyberespionage and even acts of cyberwar are occurring, but the exact scale is unclear and the financial costs are difficult to calculate because solid data is hard to get. Relying on inaccurate or unverifiable estimates is perilous, experts say, because it can tilt the country's spending priorities and its relations with foreign nations. The costs could be worse than the most dire estimates — but they could be less, too.

Computer security companies like McAfee and Symantec have stepped into the data void. Both sell anti-virus software to consumers, and McAfee also sells a range of network security products for government agencies and private companies, including operators of critical infrastructure like power plants and pipelines. Both firms conduct and publish cybercrime research, too. "Symantec is doing outstanding work on threat analysis," said Thomas Rid, a cybersecurity expert at Kings College London. "But still, of course they have a vested interest in portraying a more dangerous environment because they stand to gain for it."

The companies disagree. Sal Viveros, a McAfee public relations official who oversaw the 2009 report, said in an email to ProPublica, "We work with think tanks and universities to make sure our reports are non-biased and as accurate as possible. The goal of our papers [is] to really educate on the issues and risks facing businesses. Our customers look to us to provide them with our expert knowledge."

Symantec said its estimates are developed with standard methods used by governments and businesses to conduct consumer surveys and come from "one of the few, large, multi-country studies on cybercrime that asks consumers what forms of cybercrime they have actually experienced and what it cost them."

* * *

Cyberattacks come in many flavors. There are everyday crimes in which hackers access personal or financial information, such as credit card numbers. There are industrial crimes and espionage in which the attacker — perhaps a foreign country or company — breaks into a corporate or government network to obtain blueprints or classified information; sometimes the attacker gets inside a network and lurks there for months or years, scooping up whatever is of interest. One of the biggest categories of cybercrime is one of the least discussed — insider theft, by disgruntled or ex-employees. There's also a category of attacks that do not have overt financial motives and that can constitute acts of war: Attempts to create havoc in computer systems that control nuclear power plants, dams and the electrical grid. This category is of the greatest concern to national security officials.

One reason it's a challenge to measure the financial costs of cybercrimes is that the victims often don't know they've been attacked. When intellectual property is stolen, the original can remain in place, seemingly untouched. Even when the breach is known, how do you put a dollar value on a Social Security number, a formula for a new drug, the blueprints for a new car, or the bidding strategy of an oil firm? It may be impossible to know whether an attacker uses intellectual property in a way that causes economic harm to the victim; maybe the data isn't of much use to the attacker, or maybe the attacker, though using the data to quickly bring out a new product, is not successful in gaining market share.

There's an added complication in some attacks: Companies can be reluctant to admit they have been hacked because they fear a loss in confidence from consumers or clients. This can lead to underreporting of the problem.

"How do you even start to measure the monetary damages?" asked Nick Akerman, a partner at the law firm of Dorsey & Whitney LLP who specializes in computer cases — and one of the contributors to the McAfee report. "I would argue it is impossible. Not to say the problem isn't enormous. It is enormous. But I don't see how you can adequately come up with dollar figures."

Companies that sell security software are not bound by the same professional practices as academics, whose studies tend to refrain from sweeping estimates. Even when corporate reports involve academic researchers, the results can be suspect. Industry-sponsored studies — pharmaceuticals are an example, according to a 2003 study published by BMJ (formerly known as the British Medical Journal) — can have a bias toward the industry's economic interests. Unlike academic journals, which use a peer review process, there's no formal system of oversight for studies published by industry. The economic interest of security companies is clear: The greater the apparent threat, the greater the reason to buy their anti-intruder software. Norton, which is owned by Symantec and sells a popular suite of anti-virus software, advises in its latest cybercrime report: "Don't get angry. Get Norton."

Computer scientists Dinei Florencio and Cormac Herley, who work at Microsoft Research, the software giant's computer science lab, recently wrote a paper, "Sex, Lies and Cyber-crime Surveys," (PDF) that sharply criticized these sorts of surveys. "Our assessment of the quality of cyber-crime surveys is harsh: they are so compromised and biased that no faith whatever can be placed in their findings," their report said. "We are not alone in this judgement. Most research teams who have looked at the survey data on cyber-crime have reached similarly negative conclusions."

Julie Ryan, a professor of engineering management and systems engineering at George Washington University, co-authored a paper, "The Use, Misuse, and Abuse of Statistics in Information Security Research" (PDF). In an interview with ProPublica, she said: "From what I've seen of the big commercial surveys, they all suffer from major weaknesses, which means the data is worthless, scientifically worthless. But it's very valuable from a marketing perspective."

Yet corporate cybersurveys are repeatedly invoked; the NSA's Alexander is merely among the most prominent senior officials to do it. ProPublica provided the NSA's media office with links to critical studies, stories and blog posts about the Symantec and McAfee numbers and asked whether Alexander or the agency was aware of them or, alternately, had other data to support the numbers he cited. The NSA media office responded: "The information is publicly available and was appropriately sourced."

* * *

McAfee was founded by John McAfee, a software engineer who wrote some of the first anti-virus software in the 1980s. The company grew quickly, thanks in part to a novel marketing strategy in those days — McAfee gave away its software, charging only for tech support. The company went public in 1992 and remained a leader in its field; last year it was acquired by Intel Corp. for $7.68 billion. "We have had just one mission: to help our customers stay safe," McAfee says on its website. "We achieve this by creating proactive security solutions for securing your digital world."

In 2008, McAfee decided to commission a report that would look at how the global economic downturn was affecting data theft against companies. McAfee put one of its public relations officials, Viveros, in charge of the project. Viveros, in a phone interview, said a technology marketing company was hired to create and distribute a survey to about 1,000 information and technology executives across the globe. Purdue University's Center for Education and Research in Information Assurance and Security, headed by Spafford, analyzed the survey results, conducted follow-up interviews and helped write the report. McAfee confirmed that it helped steer $30,000 from a foundation to Purdue for the work.

The 31-page report found that the companies surveyed had an average of $12 million worth of sensitive information stored in offshore computer systems in 2008, and that each lost an average $4.6 million worth of intellectual property in 2008. The report was released on Jan. 29, 2009, in Davos, Switzerland, during a meeting of the World Economic Forum. McAfee issued a news release to announce it, and the release included dramatic numbers that were not in the report.

"The companies surveyed estimated they lost a combined $4.6 billion worth of intellectual property last year alone, and spent approximately $600 million repairing damage from data breaches," the release said. "Based on these numbers, McAfee projects that companies worldwide lost more than $1 trillion last year." The release contained a quote from McAfee's then-president and chief executive David DeWalt, in which he repeated the $1 trillion estimate. The headline of the news release was "Businesses Lose More than $1 Trillion in Intellectual Property Due to Data Theft and Cybercrime."

The trillion-dollar estimate was picked up by the media, including Bloomberg and CNET, which expressed no skepticism. But at least one observer had immediate doubts. Amrit Williams, a security consultant, wrote on his blog a few days later, "$1 trillion a year? Seriously? Where the hell did the figure come from? To give you some perspective of size the total US GDP is about 14 trillion and that includes EVERYTHING."

The news stories got the worried attention of some of the report's contributors because McAfee was connecting their names to an estimate they had no previous knowledge of and were skeptical about. One of the contributors, Augusto Paes de Barros, a Brazilian security consultant, blogged a week after the news release that although he was glad to have been involved in the report, "I could not find any data in that report that could lead into that number. ... I'd like to see how they found this number."

When the number was announced in 2009, McAfee provided no public explanation of how it was derived. "Initially we were just going to do the report, but a lot of people were asking us what was the total number, so we worked on a model," said McAfee's Viveros. This week, in response to queries from ProPublica, he disclosed details about the methodology. He said the calculations were done by a group of technology, marketing and sales officials at McAfee and were based on the survey responses.

"McAfee extrapolated the $1 trillion … based on the average data loss per company, multiplied by the number of similar companies in the countries we studied," Viveros said in an email.

The company's method did not meet the standards of the Purdue researchers whom it had engaged to analyze the survey responses and help write the report. In phone interviews and emails to ProPublica, associate professor Jackie Rees Ulmer said she was disconcerted when, a few days before the report's unveiling, she received a draft of the news release that contained the $1 trillion figure. "I expressed my concern with the number as we did not generate it," Rees Ulmer said in an email. She added that although she couldn't recall the particulars of the phone conversation in which she made her concerns known, "It is almost certainly the case that I would have told them the number was unsupportable."

Viveros said McAfee was never told by Purdue that the number could not be supported by the survey data. The company moved ahead with the news release and, Viveros noted, the trillion-dollar estimate "got a life of its own."

In February 2009, President Obama ordered a 60-day cybersecurity review to look into ways to better protect the country from cyberattacks, and he appointed Melissa Hathaway, who served as a cybersecurity adviser in the Bush administration, to oversee the effort. On May 29, Obama unveiled the review and delivered his first major cybersecurity speech. The second page of the 38-page review cited McAfee's trillion-dollar figure, and the president used it in his speech, saying, "It's been estimated that last year alone cybercriminals stole intellectual property from businesses worldwide worth up to $1 trillion."

The administration's Cyberspace Policy Review (PDF) includes footnotes, and the one for the $1 trillion estimate directs readers to McAfee's news release. It is not an ordinary occurrence that a president relies on the contents of a corporate news release to warn Americans of a major threat to the homeland's economic and national security, but Hathaway, now a security consultant, told ProPublica that at the time of the president's speech she was comfortable with McAfee's estimate because it appeared to be associated with Purdue researchers. However, she became wary of it once she began making more inquiries after the speech. "I tend not to use that number anymore," she said. "I was surprised that there wasn't proved methodology behind the number."

In March 2011, McAfee published its "Underground Economies" report, which repeated the $1 trillion estimate. Criticism of it continued, too. Robert Richardson, then director of the Computer Security Institute, skeptically wrote on the group's website in the spring of 2011 that "The trillion dollar number is just too good to kill." Later in 2011, Wired's British edition reported that "if true, the figure amounts to a massive 1.6 percent of global GDP." This year, Microsoft Research's Florencio and Herley wrote an opinion piece in The New York Times that described widely circulated cybercrime estimates as "generated using absurdly bad statistical methods, making them wholly unreliable."

These critiques have now taken on added importance because government officials are citing a variety of industry-generated numbers in their efforts to bolster support for major cybersecurity legislation. The House passed its version of a cybersecurity bill this spring; the pending Senate bill, known as the Cybersecurity Act of 2012, would enable the U.S. government and private companies to more easily share information about cyberthreats and create a set of voluntary cybersecurity standards for operators of critical infrastructure.

* * *

In his speech at the American Enterprise Institute, Gen. Alexander said Symantec placed the cost of intellectual property theft to the U.S. at $250 billion a year. Tracing the origins of this statistic — as both the U.S. Government Accountability Office (PDF) and technology writer Julian Sanchez have attempted before — is not unlike pulling a piece of yarn to unravel an old sweater. Although Symantec mentioned the $250 billion estimate in a 2011 report, "Behavioral Risk Indicators of IP Theft," the estimate is not Symantec's.

The report mentions the figure in passing, sourcing it in a footnote to a legal paper, where, as it turns out, the $250 billion number is not mentioned at all. Eric Shaw, one of two forensic psychologists Symantec retained to research the "Behavioral Risk" report, told ProPublica the footnote was a mistake. Instead, it should have referred to a different paper that points to a 2003 speech by FBI Director Robert S. Mueller. The figure is also cited in old FBI news releases available via the Internet Archive.

An agency spokeswoman said that although she believed FBI officials used a reliable source for the number, the FBI had neither developed the number nor claimed to have done so. She pointed to another document (PDF), from the U.S. Department of Justice, attributing the $250 billion figure to the Office of the U.S. Trade Representative.

Then-Commerce Secretary Gary Locke used the $250 billion number in a 2010 speech. Like Locke, the trade representative is a member of the president's cabinet; a spokeswoman for the office said the figure was not from them. "Your inquiry appears to refer to an industry-reported figure," the spokeswoman told ProPublica, pointing to a U.S. Chamber of Commerce paper on intellectual property theft. Sure enough, there's the $250 billion again — this time attributed to none other than the FBI.

There are other concerns about Symantec estimates cited by Alexander. Drawing from the 2011 Norton Cybercrime Report, Alexander put the direct cost of cybercrime at $114 billion and cybercrime's total cost, factoring in time lost, at $388 billion. The report was not actually researched by Norton employees; it was outsourced to a market research firm, StrategyOne, which is owned by the public relations giant

Edelman.

StrategyOne surveyed almost 20,000 people in 24 countries, asking them to report whether they had experienced cybercrime and how much it had cost them. The company said it used "standard research practice for online surveys" to obtain a representative sample of Internet users. To calculate a total cost, it multiplied the estimated number of victims by the average cost of cybercrime in each country.

But that still leaves room for uncertainty, several researchers told ProPublica. For example, if responses came mainly from those most concerned about cybercrime or from those who suffered the biggest losses, it could inflate the average cost. And one person's estimate of the financial damage from a cybercrime might be completely different from the next person's guess, even if both suffered the same crime and the same amount of lost time.

A StrategyOne spokesman, asked if the Symantec estimates could be called scientific, responded, "Yes, as much as any survey or poll that relies on consumers to estimate their losses based on recall."

Some experts say that's not good enough. "Nobody can really assess the true impact of cybercrime," said Franz-Stefan Gady, an analyst at a security-focused think tank called the EastWest Institute. "It's really the self-reporting — because we can't verify it. It's just as simple as that."

In their 2011 paper, Florencio and Herley of Microsoft Research did not specifically mention the Symantec or McAfee numbers. But they observed, "Far from being broadly-based estimates of losses across the population, the cyber-crime estimates that we have appear to be largely the answers of a handful of people extrapolated to the whole population."

Sen. Collins added another layer of confusion about the mysterious $250 billion figure when she spoke last week in support of the cybersecurity bill. In remarks on the Senate floor, she mentioned Gen. Alexander and said, "He believes American companies have lost about $250 billion a year through intellectual property theft."

Collins' office declined several requests for comment. A spokeswoman for Lieberman, who similarly cited Alexander and the $250 billion figure, replied, "Senator Lieberman and his staff believe that McAfee, Symantec, and General Alexander are reputable sources of information about cybersecurity."

Like this story? Sign up for our daily newsletter to get more of our best work.