Bloomberg

Cybercrime Remains Growth Industry With $445 Billion Lost

By Chris Strohm

Jun 9, 2014

Cybercrime remains a growth industry.

That's the main message from former U.S. intelligence officials, who in a report today outlined scenarios for how $445 billion a year in trade theft due to computer hackers will worsen. They warned that financial companies, retailers and energy companies are at risk from thieves who are becoming more sophisticated at pilfering data from their servers.

The outlook "is increased losses and slower growth," with no "credible scenario in which cybercrime losses diminish," according to the report published by the Washington-based Center for Strategic and International Studies. Some of the damage will be hard to trace, such as economic downturns caused by foreign competitors selling products based on stolen designs and financial markets undermined by hackers.

"Cybercrime is here to stay," said Stewart Baker, a lead author of the study who was general counsel for the National Security Agency in the 1990s and later an assistant secretary at the Department of Homeland Security.

"The real question is do we know what cybercrime is costing us?" he asked in a telephone interview.

The damage done already includes 40 million people in the U.S. having their personal information stolen within the last year and an unnamed oil company losing hundreds of millions of dollars in business opportunities when hackers obtained its oilfield exploration data, according to the report. Network security company McAfee Inc. sponsored the report for CSIS, a nonprofit Washington-based policy research organization.

Stolen Secrets

The report is intended to provide a comprehensive estimate of the cost of global hacker attacks as governments and companies fight digital incursions that could have catastrophic consequences. U.S. prosecutors in an indictment last month accused five Chinese military

hackers of stealing information from American companies that would be useful to competitors in China.

The biggest driver in the cost is stolen intellectual property, said Tom Gann, vice president of government relations for McAfee, a unit of Santa Clara, California-based chipmaker Intel Corp.

Trade secrets are stolen online by foreign governments, criminal organizations and company competitors who hire their own hackers, Gann said in a phone interview. The attacks are enabled by the growth of a sophisticated underground economy where hackers and exploitation tools can be bought using digital currencies like bitcoin.

Companies sometimes don't know their plans have been stolen.

"The man whose bicycle is stolen knows exactly what he has lost the next morning," the authors wrote. "The factory owner whose bicycle plans are stolen doesn't know he's lost anything until his competitor's bicycle reaches the market."

Market Manipulation

Hackers could break into company networks or the computers of their lawyers and accountants to steal information about pending corporate acquisitions and business strategies, the report finds.

"It is increasingly likely that the hackers will realize they can also make money in trading ahead of the plan for a merger," said Baker, who is now a partner at the law firm Steptoe & Johnson LLP.

U.S. Representative Mike Rogers, chairman of the House intelligence committee, said he too is worried about financial-market manipulation.

"We have seen nation states on our trading networks and we haven't fully answered the question what were they going to do," Rogers, a Michigan Republican, said. "Clearly, they weren't going to steal it and run. But were they going to use that to manipulate the markets?"

Business Expense

The report puts cybercrime in the context of other malicious activity, such as piracy at sea and transnational crime. It found that cybercrime costs about 0.8 percent of global gross domestic product, compared to .02 percent for maritime piracy and 1.2 percent for transnational crime.

To some degree, companies and governments accept cybercrime as a cost of doing business in the digital world, Baker said. That may not change until the costs rise above 2 percent of GDP, he said.

Trying to pinpoint the cost of hacking attacks hasn't been easy and previous estimates have varied. Keith Alexander, the former director of the NSA, said in 2012 that U.S. companies were losing $250 billion a year through intellectual property theft. He said cyber espionage constitutes the "greatest transfer of wealth in history,"

McAfee estimated in 2009 that companies lose more than $1 trillion through data theft and cybercrime. The company turned to CSIS to come up with a more accurate projection.

Cost Estimates

Estimates should be viewed with skepticism especially because the value of intellectual property can be exaggerated, said Jim Harper, a senior fellow with the Washington-based nonprofit Cato Institute.

“This kind of report probably obscures more than it informs,” Harper said in a phone interview. Not all crimes are equal.

Baker said careful economic analysis and rigor were used by CSIS to develop the cost estimate, which may be understated because many hacking attacks aren’t reported.