McAfee
An Intel Company

NET LOSSES: ESTIMATING THE GLOBAL COST OF CYBERCRIME

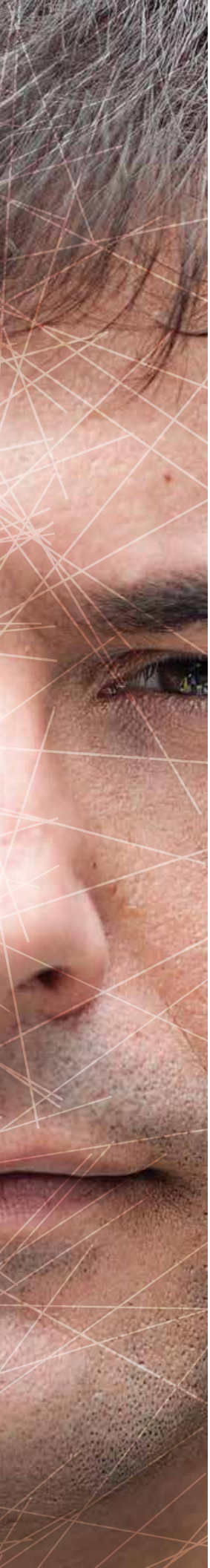
Economic impact of cybercrime II

Center for Strategic and International Studies

June 2014

Report

CONTENTS



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 $400 billion.[1] A conservative estimate would be $375 billion in losses, while the maximum could be as much as $575 billion. Even the smallest of these figures is more than the national income of most countries and governments and companies underestimate how much risk they face from cybercrime and how quickly this risk can grow.[1]

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. The cost of cybercrime includes the effect of hundreds of millions of people having their personal information stolen—incidents in the last year include more than 40 million people in the US, 54 million in Turkey, 20 million in Korea, 16 million in Germany, and more than 20 million in China. One estimate puts the total at more than 800 million individual records in 2013.[2] This alone could cost as much as $160 billion per year.[3] Criminals still have difficulty turning stolen data into financial gain, but the constant stream of news contributes to a growing sense that cybercrime is out of control.

For developed countries, cybercrime has serious implications for employment.[4] The effect of cybercrime is to shift employment away from jobs that create the most value. Even small changes in GDP can affect employment. In the United States alone, studies of how employment varies with export growth suggest that the losses from cybercrime could cost as many as 200,000 American jobs, roughly a third of 1% decrease in employment for the U.S.[5]

Using European Union data, which found that 16.7 workers were employed per million Euros in exports to the rest of the world,[6] Europe could lose as many as 150,000 jobs due to cybercrime (adjusting for national differences in IP-intensive jobs), or about 0.6% of the total unemployed.

These are not always a "net" loss if workers displaced by cyberespionage find other jobs, but if these jobs do not pay as well or better. If lost jobs are in manufacturing (and "the main engine for job creation"[7]) or other high-paying sectors, the effect of cybercrime is to shift workers from high-paying to low-paying jobs or unemployment. While translating cybercrime losses directly into job losses is not easy, the employment effect cannot be ignored.

The most important cost of cybercrime, however, comes from its damage to company performance and to national economies. Cybercrime damages trade, competitiveness, innovation, and global economic growth. What cybercrime means for the world is:

- The cost of cybercrime will continue to increase as more business functions move online and as more companies and consumers around the world connect to the Internet.
- Losses from the theft of intellectual property will also increase as acquiring countries improve their ability to make use of it 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.

Estimating Global Loss from Incomplete Data

Deciding what counts as cybercrime affects the size of any estimate. Our estimate looks at both direct and indirect costs, and data used 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. These additional indirect costs show the full effect of cybercrime on the global economy. International agreement on a standard definition of cybercrime would improve the ability to collect consistent data. That said, even a broad definition leaves out important nonmonetary effects on innovation, national defense, and the long-term competitiveness of both countries and companies.

Our sources range from the German Office for the Protection of the Constitution, the Netherlands Organisation for Applied Scientific Research (TNO), China's Peoples Public Security University, the European Commission, the Australian Institute of Criminology Research, Malaysia's Chief Technical Officer, and estimates by government agencies in other countries and consulting and cybersecurity companies around the world.

Simply listing known cybercrime and cyberespionage incidents creates a dramatic narrative. We found hundreds of reports of companies being hacked.[8] In the US, for example, the government notified 3,000 companies in 2013 that they had been hacked. Two banks in the Persian Gulf lost $45 million in a few hours.[9] A British company reported that it lost $1.3 billion from a single attack.[10] Brazilian banks say their customers lose millions annually to cyberfraud.[11] India's CERT reported that 308,371 websites were hacked between 2011 and June 2013,[12] and the Indian experience is not unique. Simply adding up the losses from the known incidents would total billions of dollars, but this provides an incomplete picture.

Most cybercrime incidents go unreported. Few companies come forward with information on losses. When Google was hacked in 2010, another 34 Fortune 500 companies in sectors as diverse as information technology and chemicals also lost intellectual property.[13] Some of the information on the incident only came to light from documents made public by WikiLeaks. Only one other company reported that it had been hacked along with Google, and it supplied no details on the effect. Similarly, when a major US bank lost several million dollars in a cyberincident it publicly denied any loss, even when law enforcement and intelligence officials confirmed it in private. Few of the biggest cybercriminals have been caught or, in many cases, even identified.

The lack of data means that any dollar amount for the global cost of cybercrime is an estimate based on incomplete data. A few nations have made serious efforts to calculate their losses from cybercrime, but most have not. This study assumes that the cost of cybercrime is a constant share of national income, adjusted for levels of development. We calculated the likely global cost by looking at publicly available data from individual countries, buttressed by interviews with government officials and experts. We looked for confirming evidence for these numbers by looking at data on IP theft, fraud, or recovery costs. In addition to a mass of anecdotes, we ultimately found aggregate data for 51 countries in all regions of the world who account for 80% of global income. We used this data to estimate the global cost, adjusting for differences among regions.

There was considerable variation in losses among countries, but this is consistent with other studies (based on surveys of individual companies), which found that companies in different countries lost different amounts per cyberincident, with US companies losing the most. Explaining these variations lies beyond the scope of this report, but one possibility is that cybercriminals decide where to commit their crimes based on an assessment of the value of the target and the ease of entry. The combination of high value, low risk, and low "work factor" (the amount of effort it takes to break into a network) makes cybercrime a winning proposition.

Not all data on cybercrime losses is of the same quality. For example, we found two divergent estimates for the European Union, one saying losses in the EU totaled only $16 billion, far less than the aggregate for those EU countries where we could find data, and another putting losses for the EU at close to a trillion dollars, more than we could find for the entire world. Japan is another interesting case. Credible survey data found that Japanese companies lost on average about half what US companies lost in hacking incidents, but if the rate of loss for Japanese companies is consistent with the rates for the US, China, or Germany, this means that the figure provided to us by officials from several ministries may underestimate the cost of cybercrime by two-thirds. The problem is even worse in the developing world, where most governments do not collect any data on cybercrime at all.

Why some nations lose more than others

One factor explaining why some nations appear to lose more than others has nothing to do with cybercrime. Differences in the thoroughness of national accounting appear to explain the variation. The alternate explanation—that some countries are miraculously unaffected by cybercrime despite having no better defenses than countries with similar income levels that suffer higher loss—seems improbable. National accounts in general need to be updated to better capture the value of intangible goods and services, and better collection of statistics on cybercrime is essential for managing this problem. Work by governments to improve the collection of data on the cost of cybercrime would make a valuable contribution to our ability to make better choices about risk, investment, and policy.

The cost of stolen Intellectual property (IP) is the most difficult to estimate for the cost of cybercrime, but it is also the most important variable for determining loss. Valuing IP is complicated, but firms place a value on IP every day. Countries where IP creation and IP-intensive industries are important for wealth creation lose more in trade, jobs, and income from cybercrime than countries that depend more on agriculture, extractive industries, or low-level manufacturing. Those countries still suffer losses from financial crime and from the theft of business confidential information on production, prices, or crop expectations that could be useful in contract negotiations, but their overall loss will be smaller than that of IP-intensive economies.

Along with the difficulty of valuing IP, other intangible losses are not easily measured. In addition to losses in business and consumer confidence, the effect of cyberespionage on national security is significant, and the monetary value of the military technology taken likely does not reflect the full cost to the nation. Underreporting and the difficulty of valuing IP are the most significant problems for estimating the cost of cybercrime. CERT Australia, for example, found that only 44% of victim companies reported the attacks,[14] and researchers in the Netherlands found a similar rate of underreporting. Many companies either don't know or won't report their losses. There are perfectly sound business reasons for this, but it produces an inherent bias towards underestimation.

A separate set of problems can be traced to the wide gap between what cybercriminals take and what they gain. This is true for both the theft of IP and many financial crimes and complicates estimation for key categories of cybercrime. We all know that a stolen bicycle may be a $500 loss for the owner and a $50 gain for the thief. The calculation is even more uncertain where cybercrime is concerned. Even if we know what was taken, in cases involving personally identifiable information or IP, criminals can't make use of all they have taken. It is harder (in some cases, much harder) to monetize the result of a successful hack than it is to the hack itself. Millions of individuals can lose their credit card data in a single incident, but only a fraction of those affected will experience financial loss.

There are wide fluctuations in available national estimates. High-income countries lost more as a percent of GDP, perhaps as much as 0.9% on

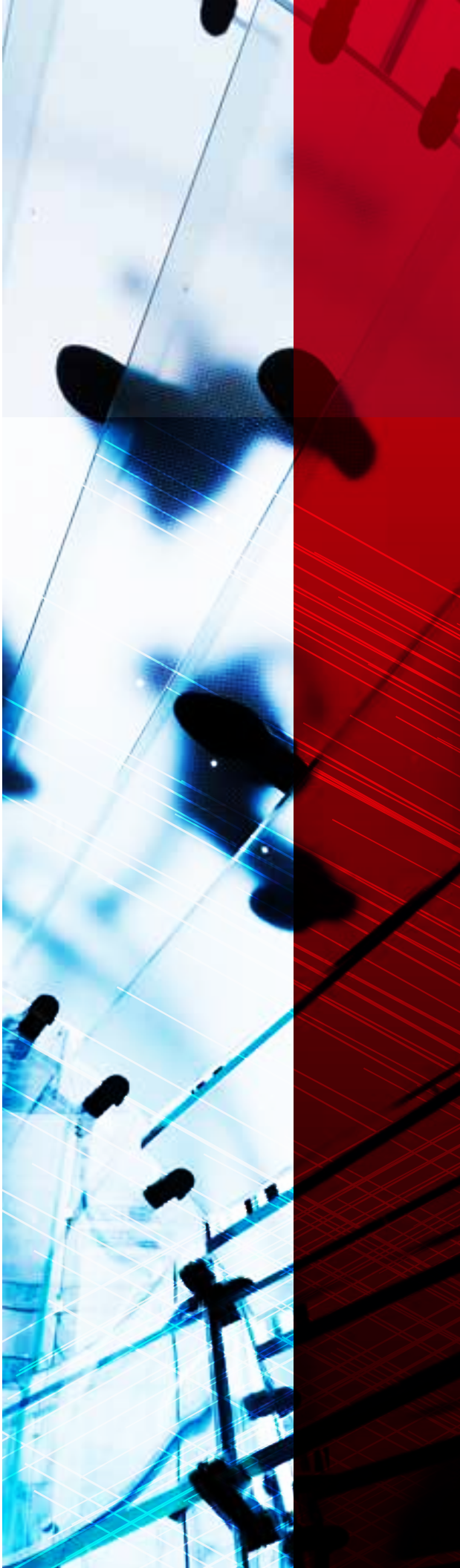
average. This may simply reflect better accounting, but rampant underreporting means that actual losses may be higher. For developing economies where IP plays a smaller economic role, the losses averaged 0.2% of GDP. The average loss among all countries for which we found data was 0.5% of GDP. Countries in Europe and North America lost more while countries in Latin American and Africa lost less. This may simply reflect better accounting in these countries, but it could also suggest that actual global losses may be higher than our estimate. The disparities we found are explained in part by the fact that the best hackers prefer to target richer countries.

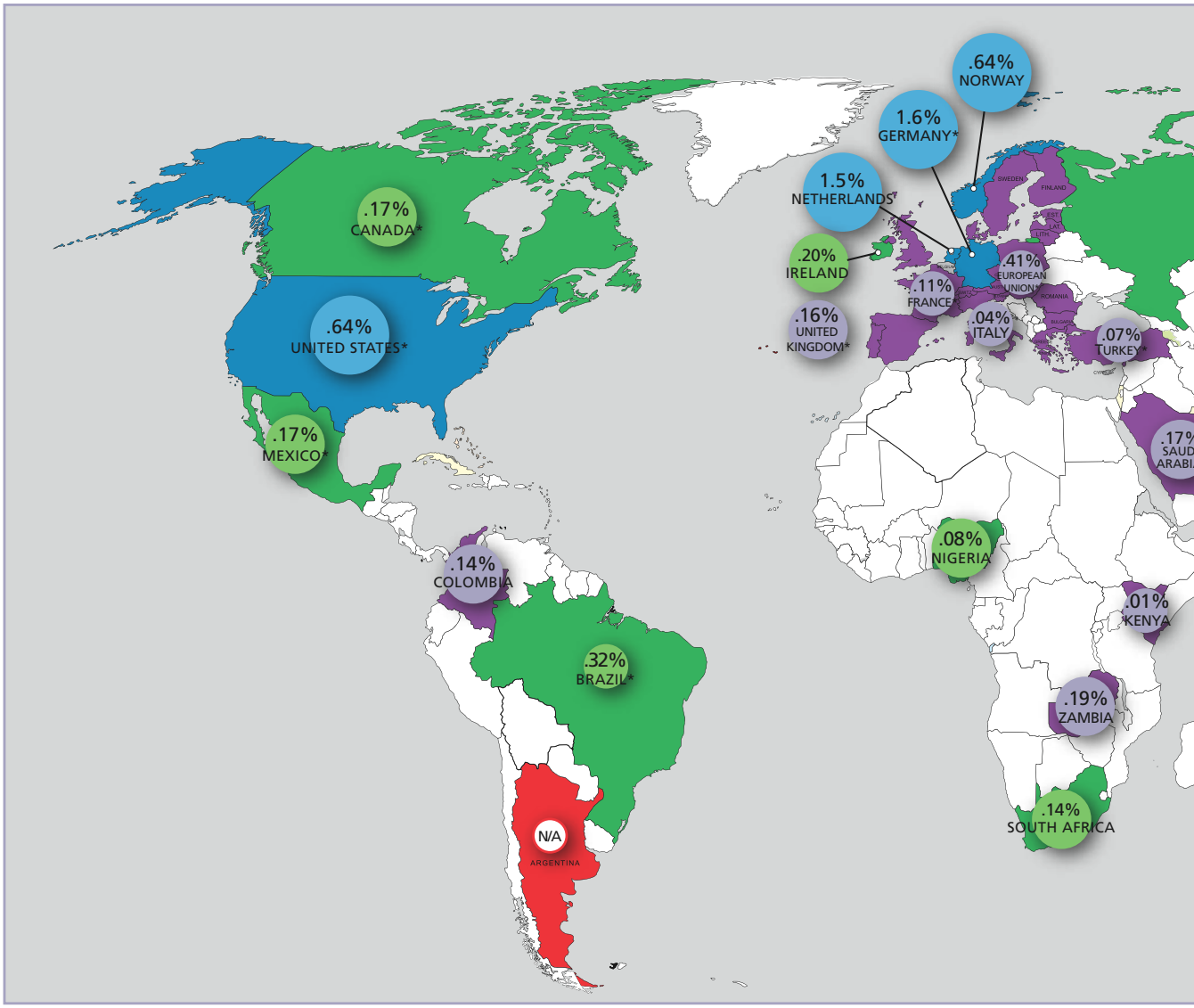
The lack of broadband connectivity also affects the amount of cybercrime—one official we interviewed said that once a country (in Africa) gets broadband connectivity, usually without adequate defenses, cybercrime spikes within a few days. The overall effect of the spike on global losses is limited, as the less developed countries do not generate the bulk of global income, but the regional effect is significant. Wealthier countries are more attractive targets for hackers but they also have better defenses. Less-developed countries are more vulnerable.

Extrapolating a global loss figure

If we used the loss by high-income countries to extrapolate a global figure, this would give us a global total of $575 billion. Another approach would be to take the total amount for all countries where we could find open source data and use it to extrapolate global costs. This would give us a total global cost of around $375 billion. A third approach would be to aggregate costs as a share of regional incomes to get a global total. This would give us an estimate of $445 billion. None of these approaches are satisfactory, but until reporting and data collection improve, they provide a way to estimate the global cost of cybercrime and cyberespionage.

Given the wide variation in estimates of loss and the difficulty of valuing IP, it is possible that we have overestimated the cost of cybercrime and cyberespionage, but the wealth of anecdotal data on the number of incidents and their effect suggests otherwise. If anything, data on crimes related to the theft of "intangible" sources of value suggest it is more likely that we have underestimated the effect. These intangible costs include the loss of military advantage by the victim country, increased military advantage for the acquiring nation, and the costs to repairing any damage. They also include increased competition for international arms sales, as the acquiring nation's products improve in quality. For example, press reports suggest that intrusion into an American advanced fighter aircraft program led to cost increases in the tens of millions of dollars and delays as software was rewritten or replaced.[15]



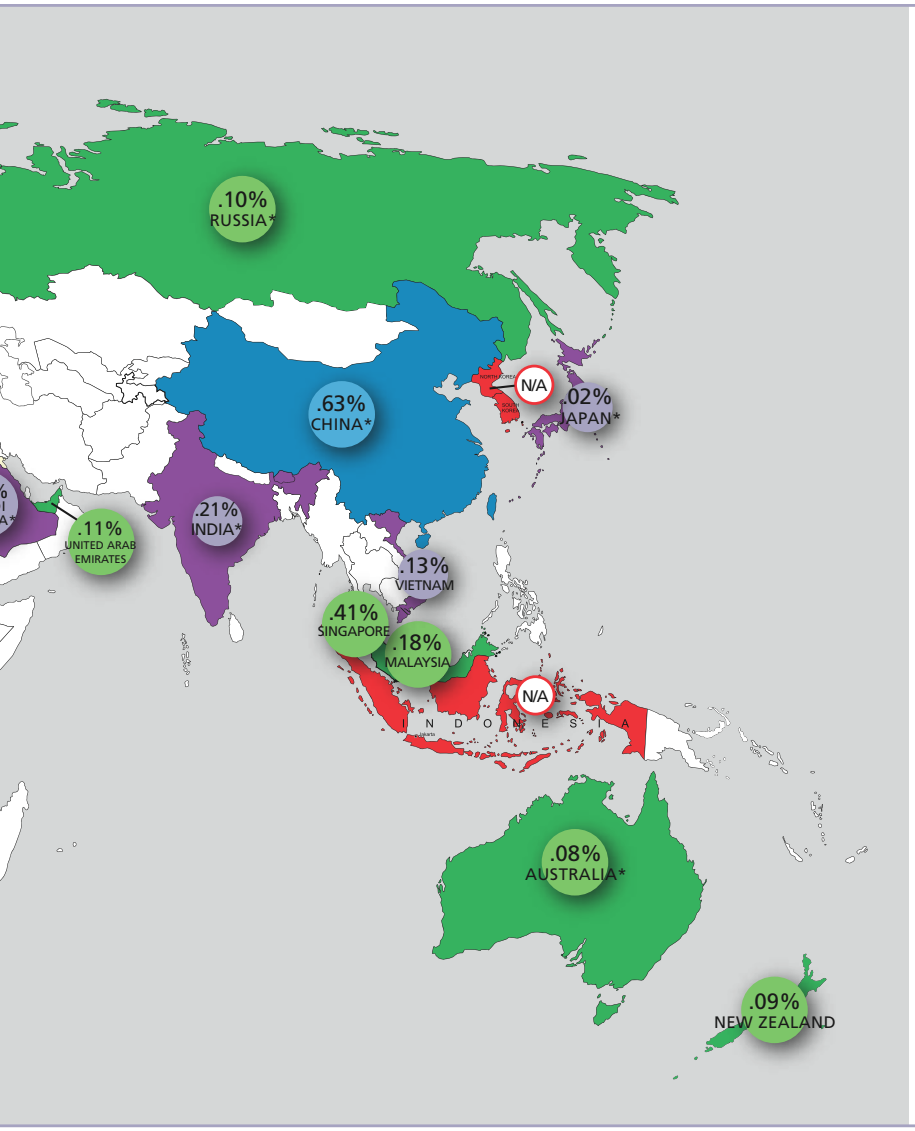


Regional Variations

Unsurprisingly, North America, Europe, and Asia lost the most, while Africa lost the least. Income levels are a good predictor of cybercrime, as wealthier countries (or firms) are more likely to be targets—it takes roughly the same amount of work to hack rich and poor targets, but rich targets produce a better return on effort.

There are strong correlations between national income levels and losses from cybercrime. It is not surprising to find that places with more money are more likely to be robbed if they are no more secure than places with less money. The best explanation is that since the risk for cybercriminals is the same whether they go after a rich target or a poor one (small in both cases), they naturally gravitate to the places where value online is highest. This may change as low-income countries increase their access and use of the Internet for commercial purposes and as cybercriminals continue to refocus their activities onto mobile platforms, the preferred source for connectivity in the developing world.

There are important variations within regions. Brazil, Mexico, and Argentina are the most affected countries in Latin America, according to the Amparo Project of the regional Internet Service Provider organization LACNIC.[16] A survey of Brazilian companies found that a third had been victims of cybercrime. Dr. Marcos Tupinamba, a Brazilian information security expert estimates that at least 5% of Brazilian companies suffer monetary losses from cybercrime; the number of



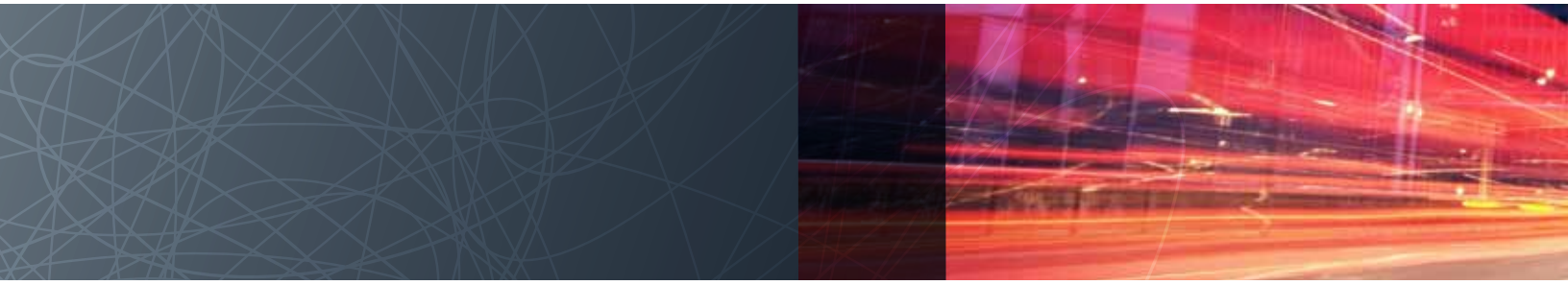
Confidence Ranking: Countries Current Tracking of Cybercrime within Their Borders.

- % **High Confidence Level**
- % **Medium Confidence Level**
- % **Low Confidence Level**
- **N/A** – Countries currently not measuring cybercrime loss
- * **G-20 Countries**

attempts is, of course, far greater. In February of 2012, a group calling itself "Anonymous Brasil" launched a denial-of-service attack, which took down a number of Brazilian financial websites, including that of Citigroup.[17] In another attack, Brazilian hackers compromised 4.5 million home DSL routers.[18] Using the hacked routers and careful social engineering, the criminals encouraged users to provide sensitive personal information or to install malware.

Like many computer-literate countries, Brazil's hacker community is active and sophisticated. Brazilian hackers' social engineering skills and the lack of security awareness among companies and consumers explains cybercrime losses in Brazil. Many experts agree that Brazil's weak laws for cybercrime and intellectual property protection means that domestic hackers, who have become increasingly professionalized, face little risk of arrest or prosecution.[19] These factors make Brazilian cybercriminals successful locally, but there is little to prevent them from turning to a global crime. Brazil also faces external cyberthreats, and information on the Brazilian economy from key crops—from soybeans to oil production—are targets.

Among high-income countries, Germany and the Netherlands had higher than average losses (as a percent of GDP). Japan and Australia had lower than average losses. This probably reflects difference in the methodologies used to calculate cost, along with difficulties in acquiring



information from companies on losses (something that officials in all countries we interviewed complained about). Japanese officials also say that the difficulty for foreign hackers to understand Japanese provided a natural layer of defense. It is easier to estimate IP losses for the US because its government has made a significant effort to identify what IP foreign hackers have taken.

Just as the G20 produces the bulk of global income, the G20 suffers the bulk of losses from cybercrime and cyberespionage. Interestingly, the rate of loss from cybercrime was roughly the same (as a percentage of GDP) among three of the four largest economies in the world (the US, China, and Germany).[20] These countries lost more than $200 billion to cybercrime. In contrast, few low-income countries had data on losses and the few where we were able to find data had small losses as a percent of national GDP. This will change as low-income countries increase their access to and use of the Internet for commercial purposes and as cybercriminals continue to refocus their activities onto mobile platforms, the preferred source for connectivity in the developing world.

Incentives Explain Cybercrime's Growth

The incentives in cybercrime are classic in that they encourage attack and discourage defense. Cybercrime produces high returns at low risk and (relatively) low cost for the hackers. The two most common exploitation techniques—social engineering, where a cybercriminal tricks a user into granting access, and vulnerability exploitation, where a cybercriminal takes advantage of a programming or implementation failure to gain access—are both surprisingly cheap. Criminals know that risk and cost are low while rewards are high. The rate of return on cybercrime favors the criminal; the incentive is to steal more. The rate of return per victim on cybercrime can be very low, but because the costs and risks of engaging in it are even lower, cybercrime remains an irresistible criminal activity.

The opposite is true for defenders. The response to cybercrime is a business decision. 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.

Several factors determine the risk that a company will be a victim of cybercrime. These include the ease of penetrating the target networks and the attractiveness of the target to hackers (determined by its value found on its networks). As people, businesses, and governments become more reliant on computer networks and devices, as more economic value is digitized and stored on networks, as manufacturing capabilities increase around the world, losses from cybercrime will grow if there is no improvement in international cooperation.

Hackers see low risk from cybercrime, with the added benefit that as manufacturing and research capabilities improve around the world, the return on stealing IP will increase, giving people more reason to hack—better indigenous manufacturing capabilities mean a greater return from hacking. Defenders lack the incentive to do more because they underestimate risk; the incentive for cybercriminals is to do more, as the rate of return is increasing. Absent a change in the incentives equation, the loss from cybercrime will increase.

Acceptable Loss from Cybercrime

Our initial report suggested that countries will tolerate malicious activity as long as it stays at acceptable levels, less than 2% of national income. If cybercrime and cyberespionage cost more than 2% of GDP, we assume it would prompt much stronger calls for action as companies and societies find the burden unacceptable. With that as a starting point, we compared losses from cybercrime to losses from other kinds of crime and mishaps to set upper and lower bounds for credible estimates of cybercrime losses. This helped us identify credible estimates.

Our May 2013 report set upper and lower "bounds" for the cost of cybercrime by comparing it to other kinds of crime and loss. We used several analogies where other organizations have quantified the costs. These provide an idea of the scope of the problem, allowing us to set a ceiling and a floor for the cost of cybercrime. Analogies are a "proxy" number rather than a direct measurement. In our first report, we looked at car crashes, maritime piracy, "pilferage," and the drug trade. The costs these imposed on society average roughly about 1% of national income. Using these analogies we decided that it was unlikely that cybercrime cost more than $600 billion, the estimated cost of the global drug trade.

One way to think about the costs of cybercrime is that societies bear the cost of crime and loss as part of doing business and a tradeoff for convenience and efficiency. Companies and individuals have decided that the net gain of using automobiles and giant merchant ships outweigh the potential cost. The problem with these analogies is that many companies do not know the extent of their losses from cybercrime, leading them to make the wrong decisions about what is an acceptable loss.

ACTIVITY	COST AS % OF GDP
Maritime Piracy	0.02% (global)
Transnational Crime	1.2% (global)
Counterfeiting/Piracy	0.89% (global
Pilferage	1.5% (US)
Car Crashes	1.0% (US)
Narcotics	0.9% (global)
Cybercrime	0.8% (global)

It is worth asking if money is the right metric. There are intangible costs that may not be captured by monetary losses. Business and consumer confidence could be one such cost, although it seems unlikely. The effect on national security is another, where the monetary value of the military technology taken likely does not reflect the full cost to the nation. In both cases, we can imagine a model that estimates how much Internet use or military investments would be worth if they were unaffected by cybercrime. Our assumption is that businesses, consumers, and governments implicitly accept a lower expected value for future cyberactivities because of the risk of loss and change or reduce their investments and activities accordingly. The question this report raises is whether those company assessments of risk are accurate or if they underestimate the effect of cybercrime.

IP Theft and Innovation Cannibalism

Cybercrime damages innovation. A company invests in research and development (R&D) to create new intellectual property (IP). They expect a certain return from their investment. If a competing product based on stolen IP appears in the market (an important qualification, as all stolen IP can be used), the expected return to the developer will be smaller than expected. In most cases, the value of research and development is the head start it gives companies in the market. New products and features attract new customers until competitors catch up. If the research is stolen, and the lead lasts only three months rather than a year, then the return on investment is a quarter of what it would have been absent cybercrime.

IP theft can range from paint formulas to rockets. The loss from IP theft is also the most difficult component of the cost of cybercrime to estimate. Valuing IP is an art form, based on estimating the future revenue IP will produce, or the value the market places on IP (which are not always the same). The actual value of intellectual property can be quite different from the research and development costs incurred in creating it. Hackers can take a company's product plans, its research results, and its customer lists, but the company may not even know that it has suffered loss.

Putting a dollar figure on IP is a normal practice in pricing a company for sale or merger. These calculations can be based on a prediction of how much future income the IP will produce or how much it would fetch if offered for sale. These estimates provide a guide for estimating loss, but companies may not know what has been taken and the cybercriminals may not be able to make full use of what they have taken. Valuing IP is one of the hardest problems for estimating the cost of cybercrime, but it is not impossible. As cybertheft of IP becomes a recognized part of the business landscape, we can expect merger and acquisition (M&A) specialists to develop better tools for evaluating both the risk of compromise and the risk of successful exploitation by competitors.

The cost to companies varies from among sector and by the ability to monetize stolen data (whether it is IP or business confidential information). Although all companies face the risk of loss of intellectual property and confidential business information, some sectors—finance, chemicals, aerospace, energy, defense, and IT—are more likely to be targeted and face attacks that persist until they succeed. Losses are higher for sectors where it is easier to monetize the stolen data, as with the chemical industry, where proprietary formulas can be easily duplicated or with sensitive business information on business negotiations. A former German intelligence official told us that "first [hackers] hollowed out our clean energy industry; now they are going after our car companies."

The most important loss from cybercrime is in the theft of IP and business confidential information, as this has the most significant economic implications. IP theft is a central problem for the information economy and not limited to cybercrime. A US Department of Commerce report found that IP theft (all kinds, not just cybercrime) costs US companies $200 to $250 billion annually.[21] The Organization for Economic Development (OECD) estimated that counterfeiting and piracy costs companies as much as $638 billion per year.[22] Hacking to steal IP is an outgrowth of two larger problems: the vulnerable nature of the Internet and weak protections for IP in many countries. Putting the two together creates a global problem. IP is a major source of competitive advantage for companies and for countries. The loss of IP means fewer jobs and fewer high-paying jobs in victim countries. The effect of IP theft is to subsidize competitors and hurt competitiveness. IP theft from cybercrime works against innovation and slows the global rate of technological improvement.

We know that balanced IP protection incentivizes growth. This is why nations have, for 150 years, put in place agreements to protect IP. Weak IP protections reduce growth and IP theft over

the Internet by increasing the scale of theft to unparalleled proportions; this both lowers and distorts global economic growth. By eroding IP protection, the effect of cybercrime is to depress the overall global rate of innovation while also reducing the ability of companies to gain the full return from their inventions, so they turn to other activities to make a profit. The impact of IP theft is not only to shift returns away from innovators, but also to reduce the overall rate of innovation. The beneficiary of IP theft grows somewhat faster, but the rest of the world grows more slowly.

Even the beneficiary of IP theft may suffer in the long run. Companies that benefit from stolen IP have less reason to invest in R&D. More importantly, they may never learn how to effectively manage R&D investments. For example, rather than invest in R&D, a company could rely on cyberespionage to gain new IP. Even if a company invests in R&D, it might use cyberespionage as a crutch if it ran into insurmountable technical problems, stealing a solution rather than creating the processes, internal research disciplines, and making the investments needed for innovation. That works until the other companies wise up or go bankrupt. A thief whose victims go broke is likely to starve along with them.

The result is to reduce returns to IP creators, since they will face competing products and get a smaller than expected revenues. A study[23] by the World Intellectual Property Organization (WIPO) found that the global IP market now produces $180 billion a year in fees and royalties. This means that the lost revenues from the theft of IP through hacking could be almost as much as the value of legitimate IP transactions. The effect of smaller returns is to diminish investment in R&D. One way to think about the cost from cybercrime is to ask how investors would react if the returns on IP and innovation were doubled.[24] Companies would invest more in R&D, and the global rate of innovation and technological improvement would increase. By eroding the returns on IP, cybercriminals hurt the victim company, but also their own country (which has less incentive to build an innovation infrastructure) and the world.

Given the nature of IP, however, this damage can be almost invisible to the victims. There is usually a delay between when IP is taken and when a competing product appears, although this varies among industry sectors. The delay between theft and production can be measured in years for technology products. Unlike the theft of a physical product, the company that created the IP is not prevented from making use of it after it has been taken, and so it cannot identify, let alone estimate, its losses. The man whose bicycle is stolen knows exactly what he has lost the next morning. The factory owner whose bicycle plans are stolen doesn't know he's lost anything until his competitor's bicycle reaches the market.

This means that companies underestimate loss and therefore underestimate their risk. Nortel's patents brought in $4.5 billion when they were sold.[25] Nortel has suffered for years from cyberespionage, with cyberspies sitting unnoticed on their networks for months at a time—this helps give an idea of the cost to an individual firm. Another firm with 800 employees had to cut its workforce in half after hackers stole its IP and a competing product appeared on the market.[26]

The limiting factor on the damage from IP theft is the ability of the acquirer to actually use the stolen technology. In the chemical sector, for example, the loss of a formula for a particular product can allow a competitor to quickly introduce a competing and potentially lower-cost product. Chemical companies are among the top targets for cybereconomic espionage. In sectors where advanced manufacturing capabilities are required, such as semiconductors or jet engines, it may be years before the theft of intellectual property produces a competing product. The value of stolen IP might be zero in the first few years only to increase dramatically when the acquirer gains the ability to use it.

One reason that the loss has been so great comes from the involvement and support of governments in the theft of IP and business confidential information. We can take as given—especially after Snowden—that nations spy on each other and have some idea of what others have been

A US Department of Commerce report found that IP theft (all kinds, not just cybercrime) costs US companies $200 to $250 billion annually. The Organization for Economic Development (OECD) estimated that counterfeiting and piracy costs companies as much as $638 billion per year.

able to extract from their national networks. When senior US cybersecurity officials say that hacking is the greatest transfer of wealth in human history, they are basing that assertion on their inside knowledge of what has been taken from American companies and been copied onto another intelligence agency's servers. Hundreds of thousands of pages of designs, business plans, blueprints, and other forms or intellectual property have been taken from companies.

Some argue that the damage from espionage is tolerable, part of the cost of doing business in the world's fastest growing markets, and that companies in developed countries can "run faster," to create new technologies and so minimize any loss. There is an economic rationale for this, in that near-term gain for an individual firm outweighs long-term costs. But several dubious assumptions underlie this defense. Illicit technology transfer, even if the technology is dated by Western standards, accelerates military modernization. It accelerates improvement in indigenous industrial and technological capabilities, making the recipient better able to absorb stolen technology and faster at creating competitive products. On a national scale, IP theft translates into damage to trade balances, national income, and jobs. The theft of IP is a kind of immediate subsidy to the acquirer and distorts trade balances and national employment. Countries, like companies, have likely underestimated the risk they face.

Penalty-Free Financial Crime

Financial crime—the theft of financial assets through cyberintrusions—is the second largest source of direct loss from cybercrime. It is a high-profile crime. When millions of people have their credit card information stolen by hackers, it gets immediate attention. Privacy laws that require reporting when personal information is compromised mean that there are numerous anecdotes of successful attacks. These attacks can cost the victim companies more than $100 million in recovery costs for large incidents, even if the actual amount gained by cybercriminals is much smaller.

The best data on cybercrime, unsurprisingly, comes from the financial sector, which is regulated, pays serious attention to cybersecurity, and can easily measure loss. In Mexico, banks lose up to $93 million annually just to online fraud.[27] The National Police Agency estimates that Japanese banks lose about $110 million annually. The 2013 hack against the US retailer Target, alone cost banks more than $200 million, and this does not count associated costs for the retailer and its customers.[28] High-profile cyberheists that garner tens of millions of dollars from banks get a lot of attention and are a global phenomenon.

Financial crime usually involves fraud, but this can take many forms to exploit consumers, banks, and government agencies. The most damaging financial crimes seek to penetrate bank networks, with cybercriminals gaining access to accounts and siphoning money. Extortion, which appears to be more common outside of North America (and is a growing crime in India—one report stated, "India appears to be the 'ransomware' capital of Asia Pacific") can involve threats to either disclose stolen information or shut down critical services if the criminal is not paid. Sometimes the payments can run into the hundreds of thousands of dollars.

Retailers are a favorite target for cybercriminals. In 2013, a series of high-loss attacks added to a list of past attacks that includes TJ Maxx, Sony, and others. UK retailers reportedly lost more than $850 million in 2013. Similar large-scale attacks have occurred against retailer, hotel chains, media companies, an airline, and financial service companies in Australia, with losses averaging more than $100 million per company. Stolen personally identifiable information (PII) and credit card data are hard to monetize, but cybercriminals appear to be getting better at this. While tens of millions of individuals have had their data compromised, the numbers of cases where these compromises have led to financial loss are lower. Cybercriminals can use the PII themselves, or they can sell it on the black market to groups who specialize in exploiting stolen information.

The theft of financial assets can be easiest to monetize, particularly when a criminal can transfer funds directly to an account they control. In other cases, cybercriminals must rely on an intermediary to monetize their crime. They use "mules" or "cashers" (low-end criminals used to monetize stolen information) to launder money, often relatives or acquaintances of the hackers, or mules can be people hired under false pretenses who think they are working for a legitimate company. The hackers will transfer funds to the mules' accounts; the mules will take a "commission" (often between 5% to 10% of the total) and forward the rest to overseas accounts. The theft of $45 million from two banks in the Middle East involved the recruitment and use of 500 mules around the world, in this case, by using cloned debit cards to withdraw money from ATMs, keep a portion for themselves, and send the rest back to the hackers.[29] Cybercriminals will drain an account, and then they access bank networks to replenish it and drain it again.[30]

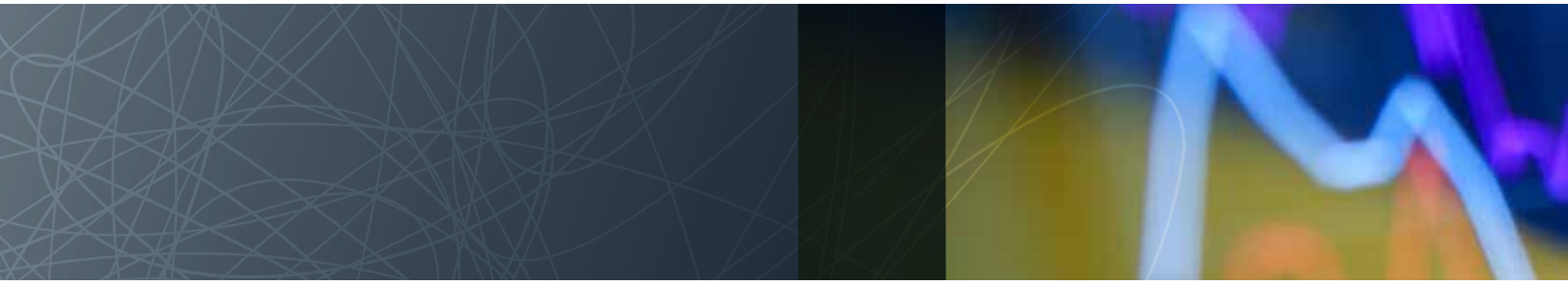
These crimes are carried out by professional gangs, some with significant organizational abilities. One European intelligence official told us that there are "20 to 30 cybercrime groups" in the former Soviet Union that have "nation-state level" capacity. These groups have repeatedly shown that they can overcome almost any cyberdefense. Financial crime in cyberspace now occurs at industrial scale.

Confidential Business Information and Market Manipulation

The theft of confidential business information is the third largest cost from cybercrime and cyberespionage. Business confidential information can be turned into immediate gain. The loss of investment information, exploration data, and sensitive commercial negotiation data can be used immediately. The damage to individual companies runs into the millions of dollars. Hacking of central banks or finance ministries could provide valuable economic information on the direction of markets or interest rates.

One European company told of going to negotiate a contract only to find that the other side already knew their bottom line. The company later discovered that it had been hacked. The CEO of a major oil company said privately that the loss of oilfield exploration data by hacking cost the company hundreds of millions of dollars. The director of a European security service described cyberespionage as a "normal business practice" in some parts of the world.[31]

One example would involve the theft of sensitive negotiating data that would give one party an advantage in a business deal. One UK company told British officials that it incurred revenue losses of $1.3 billion through the loss of intellectual property and disadvantages in commercial activities.



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. If our estimates are right, cybercrime extracts between 15% and 20% of the value created by the Internet.

Anecdotes about loss come from every major economy. In 2010, three leading Australian mining firms were hit by cyberattacks that disrupted operations and, in one instance, were used to gain confidential information related to major contract negotiations.[32] Australian authorities said there were more than 200 attempts to hack into one mining company's networks that began with the onset of contract negotiations and continued for their duration. Similar stories from companies in the US, Europe, Asia, and Latin America are easy to find. Loss of client information is the biggest cost involved for Indian companies.[33] A BBC report found that cybercrime could cost Indian companies as much as 5% of their profits.[34]

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 (which can sometimes be an easier target), cybercriminals can acquire inside information on acquisition and merger plans, quarterly revenue reports, or other data that could affect a company's stock prices. Criminals taking advantage of this information for trading could be hard to detect, as it might look like a normal trade, especially if it was carried out in another stock market. Using chat rooms and social media for "pump and dump," is a well-established technique, with criminals providing false information about a company's prospects and then cashing in when the market reacts. Turkey's financial regulators, for example, found suspicious activity intended to manipulate markets and stock prices that went beyond "pump and dump" schemes.[35] For high-end cybercriminals, cybercrime may be morphing into financial manipulation that will be exceptionally difficult to detect.

Opportunity Cost and Cybercrime

Opportunity cost is the value of forgone activities—opportunities or benefits that cannot be realized because resources have been expended elsewhere. Three kinds of opportunity costs determine the losses from cybercrime: reduced investment in R&D, risk averse behavior by businesses and consumers that limits Internet use, and increased spending on network defense.

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 for using an inherently insecure network. The rate at which spending on cybersecurity increases reflects not only an increased use of network technologies, but also an increased awareness of the threat. We can use the rate of change in cybersecurity spending as an indicator of opportunity cost and a "risk premium." For example, if companies spent $1 dollar in 2011 on cybersecurity, they increased this to $1.15 in 2012. By comparison, companies spend much less than 1%[36] of the total values of shipping to protect themselves from maritime piracy.

Another way to look at the opportunity cost of cybercrime is to see it as a share of the Internet economy. Studies estimate that the Internet economy annually generates between $2 trillion and $3 trillion,[1] a share of the global economy that is expected to grow rapidly. If our estimates are right, cybercrime extracts between 15% and 20% of the value created by the Internet, a heavy tax on the potential for economic growth and job creation and a share of revenue that is significantly larger than any other transnational criminal activity.

A survey done for this study found that the total addressable market (a measure of market size) for cybersecurity products and services has increased by 8.7% since 2011, from $53 billion to $58 billion in 2013 (see Appendix B). Business demand for cybersecurity products increased by 14.7% in the same period, and consumer demand increased by 10.7%. Much of this growth is the result of the increased awareness of cybersecurity risks among firms. As awareness of cyberrisks grows, companies can better assess risk and spend more to manage, but if the problem were getting smaller, the market would be shrinking. Companies will keep spending to secure their networks no matter what, but smart companies realize they must spend more than they would otherwise. The real cost is measured by looking at the additional amount they have to spend. Judging from the growth in cybersecurity spending, this could be $10 billion more annually in addition to the monetary losses from cybercrime.

Cybercriminals do not always seek to extract value from their attacks. A cybercriminal can use an Internet attack to disrupt the provision of a key service. We saw this in 2012, when criminals permanently erased the data from 30,000 computers at a large oil producer and launched similarly disruptive attacks against South Korean banks and media outlets that also erased the data on thousands of hard drives.[37] These companies and their customers experienced harm that went beyond the cost of cleaning up and repair. The threat of service disruption can be part of an extortion scheme or a potential area of risk for some critical infrastructure.

Numerous surveys of companies have also found that the cost of recovering from cyberattacks, including reputational damage, where the trust in a company decreases and their brand loses value, is also increasing.[38] A 2012 survey estimated, based on the value that victims of cybercrime placed on time lost due to the incident, that this amounted to an additional $274 million to the hacked company.

The opportunity cost arising from the failure to take full advantage of information technology is harder to measure. The use of IT in healthcare has been slowed by the fear, valid or not, that health information could be stolen, patient data could be manipulated, and devices interfered with by hackers. The same may prove to be true for self-driving automobiles and other valuable technologies.

Recovery Costs

Cleaning up in the aftermath of cybercrime is expensive, often more expensive than the crime itself. The cost to individual companies of recovery from cyberfraud or data breaches is increasing. While we know criminals will not be able to monetize everything that they steal, the victim has to spend as if they could monetize all the data or PII that was taken. As with spending on security, the aggregate cost to nations may be higher than monetary losses or 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.[39] The effect on a business can include damage to brand and other reputational losses and harm to customer relations and retention. In the UK, 93% of large corporations and 87% of small businesses reported a cyberbreach in the past year, with a breach estimated to cost large companies as much as $1.4 million and small companies more than $100,000.[40] The cost of the cleanup of a cyberincident is made public in many cases. The range of expenditures can be great (from $3 million for the State of Utah to $171 million for Sony Corporation). One estimate puts the losses to the retail chain, Target, as up to $420 million, including reimbursement, the cost of reissuing millions of cards, legal fees, and credit monitoring for millions of customers.[41]

Companies experience reduced valuation after they have been hacked. The effect on stock prices can be significant—a fall in value of between 1% and 5%—but the decline is not permanent, and prices usually recover within a quarter or two. This stock price recovery may change in the future if companies are required to report major hacking incidents and describe what has actually been lost. There is also a possibility best practices and standards of care for cybersecurity become more common, companies may face increased liability and lawsuits over a lack of due diligence.[42]

The Future: Storms Ahead, and Continued Growth for Cybercrime

If this were a static situation, we could say that cybercrime is just another social ill, diverting at most an eighth of a percent of global income from legitimate to illegal activities. This picture is wrong. First, as more business activities move online and as more consumers around the world connect to the Internet, and as autonomous devices are connected ("the Internet of things"), the opportunities for cybercrime will grow. Cybercrime remains a growth industry. Second, losses stemming from the theft of IP will also increase as acquiring countries improve their ability to make use of it to produce competing goods.

This means that companies that fail to adequately protect their networks will be at an increasing competitive disadvantage. There are also costs to nations in jobs and trade balances, and a global cost as cybercrime slows the pace of global innovation by reducing the rate of return to innovators and investors. Countries that can't strengthen their cyberdefenses will be at a disadvantage. Over time, if nothing else changes, losses from cybercrime will grow.

Predicting the future becomes a comparison of probabilities—the probability of improved defense and better international cooperation compared to the probability of increased development around the world. The latter is certain; the former remain an area for additional work. It seems safe to say that even if the level of loss from financial crime remains constant, the level of loss from IP theft can only increase.

The situation is not irreparable, however, and it is worth asking what would change this picture. Better technology and stronger defenses could reduce the loss from cybercrime. Agreement and application of standards and best practices for cybersecurity could also reduce the cost of cybercrime. International agreement on law enforcement and on state behavior that included restraints on crime could also reduce losses, particularly if this included agreement to observe existing international commitments (such as World Trade Organization [WTO] commitments to protect IP). Making progress on these changes will require governments to do a better job accounting for loss and companies to do a better job assessing risk. These are well within the realm of the possible if people decide to treat cybercrime seriously and take action against it.

Absent these changes, we think there are two possible outcomes. In the first, the cost of crime for developed countries would stay largely flat, at least as a percentage of GDP, but the global cost would increase as new entrants and developing countries accelerate their use of the Internet. In the second, the cost to developed economies would increase as even more activities move online and as hackers improve their ability to monetize what they can steal. We do not see a credible scenario in which cybercrime losses diminish. The outlook for the world is increased losses and slower growth.

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/

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

Appendix A: Economic Impact of Cybercrime

Brazil has been undergoing profound changes in the last 30 years, with the democratization of the country in the 1980s, inflation stabilization during the administration of President Fernando Henrique Cardoso in the 1990s, and more recently with social policies that were expanded in the 2000s during the administration of President Luiz Inácio Lula da Silva and were started in the previous government.[43]

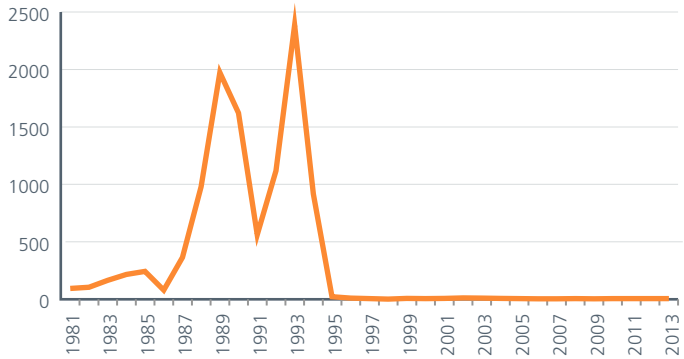
Today Brazil is one of the largest economies in the world (in 2012, it was seventh largest, behind only the US, China, Japan, Germany, France, and the UK), the largest in Latin America (its GDP is 40% of the GDP in Latin America), and is part of the group of emerging countries known as BRICS (Brazil, Russia, India, China, and South Africa). The Brazilian population, with almost 200 million people, is the fifth largest in the world (behind only China, India, the US, and Indonesia) and the largest in Latin America (34% of the population of Latin America).[44] The unemployment rate in Brazil is low (5.4% in 2013),[45] and there is a very strong social mobility, where the poorest segment of society (classes D and E) decreased from 55% of the population in 2003 to 34% in 2011. The middle class (class C) increased from 37.5% to 54% of the population in the same period, and the wealthier classes (A and B) also increased from 7.5% to 12.0%.[46]

With the dramatic growth of the Brazilian economy, very large population, low unemployment, and social mobility, most Brazilians are Internet users and cybercrime is now rampant. According to 2012 data, more than 88 million Brazilians were users of the Internet, which accounts for more than 45% of the population.[47] In comparison, the percentage of the population of Latin American Internet users is 43% (which corresponds to 10.5% of the world population of Internet users), and 34% of the world population of Internet users. Comparing absolute numbers, Latin America had nearly 255 million users in 2012, 32% of them Brazilians. North America had nearly 274 million users (78.6% of the US population). Another important factor is the increase in the percentage and number of Internet users in Latin America—18 million people in 2000 to almost 255 million in 2012, which represent 1300%.[48]

Given this scenario, with all the economic improvements that have occurred over the years, the country is also wrestling with the problem of cybercrime. Today, cybercrime is one of the top four economic crimes in the world. In Brazil, cybercrime is in second place.[49] According to data from FEBRABAN (Brazilian Federation of Banks), Brazil had losses of R $1.4 billion in 2012 (US $591 million),[50] down 6.7% over the previous year. It is also important to note that although the absolute number is impressive, it represents only 0.06% of bank transactions.[51] It reflects, among other factors, weak laws and lack of awareness among businesses and consumers on this subject. According to the *Global Economic Crime Survey 2011—Brazil*, 40% of Brazilian respondents said they had never received any training in cybersecurity, 57% of Brazilian companies said they do not have the resources to fight cybercrime or know if they are capable of cybercrime investigatations, and 50% of Brazilians said they didn't know that their companies could detect and prevent cybercrime.[52]

Brazil lived with hyperinflation during the 1980s and into the early 1990s, and this reached its peak with inflation of nearly 2,500% in 1993 (Graph 1),[53] the year before the implementation of the Real Plan, which put an end to the serious economic problems that plagued the country for so long. On this issue of hyperinflation, both the government and the financial system were forced to make changes. One of the key changes was that financial institutions embraced electronic systems and online banking.[54]

Graph 1: Inflation in Brazil (%)



According to the *2013 BSA Global Cloud Computing Scorecard*, because Brazil had been struggling with the cybersecurity issue for a while, it adopted modern laws against cybercrime, but most of these measures are inadequate. In Brazil, where organized crime is rife and laws to prevent cybercrime are few and ineffective, the country is becoming a laboratory for cybercrime, with hackers committing crimes such as identity and data theft, credit card fraud, and piracy, as well as online vandalism. According to the mi2g Intelligence Unit, a digital risk consulting firm in London, several notorious groups of vandals and Internet criminals originated in Brazil.[55]

According to the Business Software Alliance (BSA), existing criminal laws in Brazil are out of compliance with international standards for digital crime. Brazil has gaps in the protection of intellectual property and has not signed the WIPO Copyright Treaty, an international treaty on copyright law adopted by the member states of the World Intellectual Property Organization (WIPO). Brazil needs to create strong laws to end impunity for hackers, promote good data management, and encourage the growth of e-commerce.[56] This is currently under discussion in the Brazilian National Congress through the Marco Civil da Internet, which will establish a "constitution" of the global network of computers in Brazil, with rights and duties of users and companies.[57]

Appendix B: Total Addressable Market for Cybersecurity

PRODUCT AREAS	2011	2012	2013	% CHANGE 2011–2013
Email Gateway	2414	2447	2622	8.6%
Next Generation Firewall	2249	2721	3217	43.0%
Intrusion Prevention Systems	1890	1859	1906	0.8%
Firewall	2356	2631	2576	9.3%
VPN	941	725	746	-20.7%
Web	1914	1991	2122	10.9%
Total IAM	4019	4418	4860	20.9%
Corporate Endpoint	3225	3447	3692	14.5%
Consumer	4451	4638	4916	10.4%
Vulnerability Assessment	837	916	1008	20.4%
Forensics	221	305	369	67.0%
Proactive Endpoint Risk Management	465	482	506	8.8%
SIEM	1308	1434	1594	21.9%
Policy and Compliance	801	875	962	20.1%
Security Device Systems Management	201	179	166	-17.4%
Consulting Services		4366	4694	7.5%
Integration Services		8109	8529	5.2%
Managed Security Services Subtotal		9659	11274	16.7%
Education and Training Subtotal		1605	1699	5.9%
Other Security (2012)	758	773	810	6.9%
TOTAL SECURITY (PRODUCT/SERVICES)				
Total Available Market		53611	58267	8.7%
Total Security Product Total Available Market	28048	29872	32071	14.3%
Total B2B Product Total Available Market	23597	25233	27155	15.1%

Appendix C: Cybercrime as a Percent of GDP

COUNTRY	% OF GDP	CONFIDENCE	G-20 COUNTRIES
Argentina	N/A		
Australia	0.08%	M	X
Brazil	0.32%	M	X
Canada	0.17%	M	X
China	0.63%	H	X
Colombia	0.14%	L	
EU	0.41%	L	X
France	0.11%	L	X
Germany	1.60%	H	X
India	0.21%	L	X
Indonesia	N/A		
Ireland	0.20%	M	
Italy	0.18%	L	
Japan	0.02%	L	X
Kenya	0.01%	L	
Korea	N/A		
Malaysia	0.18%	M	
Mexico	0.17%	M	X
Netherlands	1.50%	H	
New Zealand	0.09%	M	
Nigeria	0.25%	M	
Norway	0.64%	H	
Russia	0.10%	M	X
Saudi Arabia	0.17%	L	X
Singapore	0.41%	M	
South Africa	0.14%	M	
Turkey	0.07%	L	X
United Arab Emirates	0.11%	M	
United Kingdom	0.16%	L	X
United States	0.64%	H	X
Vietnam	0.13%	L	
Zambia	0.19%	L	

Appendix D: Select Bibliography on Cybercrime

"Internet Value Chain Economics," AT Kearney, last modified May 2010, Last Accessed: 2/10/2014, http://www.atkearney.com/paper/-/asset_publisher/dVxv4Hz2h8bS/content/internet-value-chain-economics/10192.

Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michel J.G. van Eeten, Michael Levi, Tyler Moore, Stefan Savage, "Measuring the Cost of Cyber Crime" (paper presented at the Weis 202 Workshop on the Economics of Information Security Berlin, Germany, June 25-26, 2012), Last Accessed 2/10/2014, http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf.

Dennis Blair, Jon Huntsman Jr., Craig Barrett, Slade Gordon, William J. Lynn III, Deborah Wince-Smith, Michael K. Young, "The IP Commission Report: The Report on the Commission of the Theft of American Intellectual Property," (Seattle, Washington, National Bureau of Asian Research: 2013), Last Accessed: 2/10/2014, http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

Brian Cashell, William D. Jackson, Mark Jickling, Baird Webel, "The Economic Impact of Cyber-Attacks," (Washington, D.C., Congressional Research Service: 2004), Last Accessed: 2/10/2014, http://congressionalresearch.com/RL32331/document.php.

DAKA Advisory, "Meeting the cyber security challenge in Indonesia: An analysis of threats and responses," (Jakarta, Indonesia, British Embassy in Indonesia, 2013), Last Accessed: 2/10/2014, http://dakaadvisory.com/wp-content/uploads/DAKA-Indonesia-cyber-security-2013-web-version.pdf.

Financial Action Task Force, "Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems," (Paris, France Financial Action Taskforce OECD: 2008), Last Accessed: 2/10/2014, http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20TF%20Vulnerabilities%20of%20Commercial%20Websites%20and%20Internet%20Payment%20Systems.pdf.

Dinei Florêncio, Cormac Herley, "Sex, Lies, and Cyber-crime Surveys," Microsoft Research (2013), Last Accessed: 2/10/2014, http://research.microsoft.com/pubs/149886/sexliesandcyber crimesurveys.pdf.

Hogans Lovells International LLP, "Report on Trade Secrets for the European Commission," (Brussels, Belgium, Hogans Lovells International LLP: 2013), Last Accessed: 2/10/2014, http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/120113_study_en.pdf.

International Telecommunications Union, "Understanding Cyber Crime: Phenomena, Challenges, and Legal Response," (New York, N.Y., I.T.U.: 2012), Last Accessed: 2/10/2014, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cyber crime%20legislation%20EV6.pdf.

KPMG International, "Cyber Crime – A Growing Challenge for Governments," Issues Monitor 8 (2011), Last Accessed: 2/10/2014, http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf.

William Lehr, "Measuring the Internet: the Data Challenge," OECD Digital Economy Papers No. 194 (2012), Last Accessed: 2/10/2014, http://www.oecd-ilibrary.org/docserver/download/5k9bhk5fzvzx.pdf?expires=1392049778&id=id&accname=guest&checksum=9751668C60F33441C4BB7B4B04712747.

Avner Levin, Daria Ilkina, "International Comparison of Cyber Crime," (Toronto, Canada, Ryerson University: 2013), Last Accessed: 2/10/2014, http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_International_Comparison_ofCyber_Crime_-March2013.pdf.

James A. Lewis, Stewart Baker, "Estimating the Cost of Cyber Crime," Center for Strategic and International Studies, Washington, D.C., June 2013), Last Accessed: 2/10/2014, https://csis.org/event/estimating-cost-cyber-crime-and-cyber-espionage.

Emma McClarkin, "Cyber Crime- New Investigation Strategies and New Technologies," (Brussels, Belgium, Special Committee on Organized Crime, Corruption, and Money Laundering: 2012), Last accessed: 2/10/2014, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/crim/dv/mcclarkin_/mcclarkin_en.pdf.

Norton by Symantec, "2012 Norton Cyber Crime Report," (Mountain View, CA, Symantec: 2012), Last Accessed: 2/10/2014, http://now-static.norton.com/now/en/pu/images/Promotions/2012/cyber crimeReport/2012_Norton_Cyber crime_Report_Master_FINAL_050912.pdf.

Ponemon Institute, "2013 Cost of Data Breach Study: Global Analysis," (Traverse City, Michigan, Ponemon Institute: 2013), Last Accessed: 2/10/2014, http://www.symantec.com/content/en/us/about/media/pdfs/b-cost-of-a-data-breach-global-report-2013.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2013Jun_worldwide_CostofaDataBreach.

TrendMicro, "Latin America and Caribbean Cybersecurity Trends and Government Responses," (Washington, D.C., Organization of American States: 2013), Last Accessed: 2/10/2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf.

United Nations Office on Drugs and Crime, "Comprehensive Study on Cyber Crime," (New York, N.Y., United Nations: 2013), Last Accessed 2/10/2014, http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBER CRIME_STUDY_210213.pdf.

The Australian Business Assessment of Computer User Security (ABACUS) survey: methodology report, http://www.aic.gov.au/publications/current%20series/rpp/100-120/rpp102.html.

Latin American and Caribbean Cybersecurity Trends and Government Responses http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf, http://www.welivesecurity.com/wp-content/uploads/2014/01/informe_esr13.pdf.

Information Security in Swiss Companies: A Survey on Threats, Risk Management and Forms of Joint Action, http://www.css.ethz.ch/policy_consultancy/products_INT/DetailansichtPubDB_EN?rec_id=1396.

Impact of cyber crime on businesses in Canada, https://www.icspa.org/media/icspa-news/icspa-news-publications/article/icspa-releases-study-to-measure-the-impact-of-cyber-crime-on-businesses-in-canada-43/abp/3/.

Data Breaches: Greater frequency, Greater Costs for All Companies, http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf.

Tim Stapleton, Zurich National, "Data Breaches: Greater frequency, Greater Costs for All Companies," http://www.zurichna.com.

Trustwave, 2013 Global Security Report, http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf.

Rutger Leukfeldt, Sander Veenstra & Wouter Stol, "High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands," NHL University of Applied Sciences, The Netherlands, June 2013.

National Cyber Security Centre, Ministry of Security and Justice, "Cyber Security Assessment Netherlands CSAN-3," June 2013.

[1] Which reached $72 trillion in 2012.

[2] John Hawes, "2013 An Epic Year For Data Breaches With Over 800 Million Records Lost," *Naked Security*, February 19, 2014, http://nakedsecurity.sophos.com/2014/02/19/2013-an-epic-year-for-data-breaches-with-over-800-million-records-lost/

[3] http://www.ponemon.org/news-2/23

[4] While a subject of debate, economist Arthur Okun found that for every 1% increase in unemployment, GDP will be roughly 2% lower.

[5] International Trade Administration, "Jobs Supported by Exports: An Update," March 12, 2012, http://www.trade.gov/mas/ian/build/groups/public/@tg_ian/documents/webcontent/tg_ian_003639.pdf

[6] N. Sousa, J. M. Rueda-Cantuche, I. Arto, and V. Andreoni, "Extra: EU Exports and Employment," *Chief Economists Note, European Commission, Trade,* Issue 2, 2012, http://trade.ec.europa.eu/doclib/docs/2012/may/tradoc_149511.%202_24.05.2012.pdf. See also: "Unemployment Statistics," *European Commission: Euro Stat*, http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Unemployment_statistics; epp.eurostat.ec.europa.eu/cache/.../3-31012014-AP-EN.PDF

[7] "Extra - EU Exports and Employment," trade.ec.europa.eu/doclib/html/149511.htm

[8] Statement by Dennis McDonough at the White House.

[9] "Six Arrested Over 45 Million Cyber Heist on Middle East Banks," *Al Arabiya*, November 19, 2013, http://english.alarabiya.net/en/business/banking-and-finance/2013/11/19/Six-arrested-over-45-million-cyber-heist-on-Middle-East-banks.html

[10] Tom Whitehead, "Cyber Crime A Global Threat, MI5 Head Warns," *The Telegraph*, June 6, 2012, http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/9354373/Cyber-crime-a-global-threat-MI5-head-warns.html

[11] Jordan Robertson, "Why Are Hackers Flooding Into Brazil?" *Bloomberg*, September 13, 2013, http://www.bloomberg.com/news/2013-09-13/why-are-hackers-flooding-into-brazil-.html

[12] Pavan Duggal, "The Face of Indian Cyber Law in 2013," *The Business Standard*, December 30, 2013, http://www.business-standard.com/article/technology/the-face-of-indian-cyber-law-in-2013-113123000441_1.html

[13] Notable companies include Yahoo, Symantec, Adobe, Northrop Grumman, and Dow Chemical. See: Ariana Eunjung Cha and Ellen Nakishima, "Google China Cyberattack Part of Vast Espionage Campaign, Experts Say," *The Washington Post*, January 14, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html

[14] "Cyber Crime and Security Survey Report 2012," *CERT Australia*, https://www.cert.gov.au/system/files/614/679/Cyber%20Crime%20and%20Security%20Survey%20Report%202012.pdf: 5

[15] http://defensetech.org/2012/02/06/did-chinese-espionage-lead-to-f-35-delays/; http://breakingdefense.com/2013/06/top-official-admits-f-35-stealth-fighter-secrets-stolen/

[16] Patricia Prandini and Marcia L. Maggiore, "Panorama del ciberdelito en Latinoamérica," *Project Amparo*, June 2011, http://www.proyectoamparo.net/files/LACNIC-PanoramCiberd-VsFinal-20110701.pdf: 72

[17] Gerald Jeffris, "Citi Hit in Brazilian Hacker Attack," *The Wall Street Journal*, February 4, 2012, http://online.wsj.com/news/articles/SB10001424052970203889904577200964142208498

[18] Dan Goodin, "DSL modem hack used to infect millions with banking fraud malware," *Ars Technica*, October 1, 2012, http://arstechnica.com/security/2012/10/dsl-modem-hack-infects-millions-with-malware/

[19] For example, Business Software Alliance, http://www.forbes.com/sites/ricardogeromel/2012/03/02/hackers-stole-1billion-in-brazil-the-worst-prepared-nation-to-adopt-cloud-technology/, also PWC, *Global Economic Crime Survey 2011—Brazil*

[20] Incomplete figures for Japan were provided in interviews with Japanese officials from NISC, NPA, and METI.

[21] "Stolen Intellectual Property Harms American Businesses Says Acting Deputy Secretary Blank," *The Commerce Blog, U.S. Department of Commerce*, November 29, 2011, http://www.commerce.gov/blog/2011/11/29/stolen-intellectual-property-harms-american-businesses-says-acting-deputy-secretary-

[22] Robert J. Shapiro and Kevin A. Hassett, "The Economic Value of Intellectual Property," *Sonecon,* http://www.sonecon.com/docs/studies/IntellectualPropertyReport-October2005.pdf: 3

[23] *World Intellectual Property Report 2011—The Changing Face of Innovation*

[24] Ibid.

[25] Alastair Sharp, "Apple/RIM Group Top Google in $4.5 Billion Nortel Sale," *Reuters*, July 1, 2011, http://www.reuters.com/article/2011/07/01/us-nortel-idUSTRE7600PF20110701

[26] "Trade Secrets: Supporting Innovation, Protecting Know-How," *European Commission Conference*, June 29, 2012, http://ec.europa.eu/internal_market/iprenforcement/docs/conference20120629/ts_summary_consolidatedfinal20120913_en.pdf

[27] University of Pennsylvania Wharton School of Business, "Latin American Reaches a Crossroads for Guarding Against Cyber Crime," July 24, 2013, http://www.wharton.universia.net/index.cfm?fa=viewfeature&id=2384&language=english

[28] "Target Data Breach Cost for Banks Tops $200M," *Associated Press*, February 18, 2014, http://www.nbcnews.com/business/business-news/target-data-breach-cost-banks-tops-200m-n33156

[29] Jessica Dye, Joseph Axe, and Jim Finkle, "Huge cyber bank theft spans 27 countries," *Reuters*, May 9, 2013, http://www.reuters.com/article/2013/05/09/net-us-usa-crime-cyber crime-idUSBRE9480PZ20130509; "Six Arrested Over 45 Million Cyber Heist on Middle East Banks," *Al Arabiya*, November 19, 2013, http://english.alarabiya.net/en/business/banking-and-finance/2013/11/19/Six-arrested-over-45-million-cyber-heist-on-Middle-East-banks.html

[30] http://krebsonsecurity.com/2013/11/feds-charge-calif-brothers-in-cyberheists/

[31] "The Olympics and Beyond," *Address at the Lord Mayor's Annual Defence and Security Lecture by the Director General of the Security Service, Jonathan Evans*, June 25, 2012, https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/the-olympics-and-beyond.html

[32] "Chinese Cyber Attack on BHP Billiton, Rio Tinto, and Fortescue Metals Group," *News.com.au*, April 20, 2010, http://www.news.com.au/finance/chinese-cyber-attacks-on-bhp-billiton-rio-tinto-and-fortescue-metals-group/story-e6frfm1i-1225855748114; Jennifer Hewett, "Miners fear secrets stolen by Chinese cyber-spies," *The Australian*, April 20, 2010, http://www.theaustralian.com.au/business/mining-energy/miners-fear-secrets-stolen-by-chinese-cyber-spies/story-e6frg9df-1225855718533; interview with Australian Federal Police

[33] Zahra Khan, "India Tops Cyber Crime Hit List," *The Live Mint*, November 20, 2013, http://www.livemint.com/Specials/ZrC70l3QsLMihkFbAfoL7O/India-tops-cyber crime-hit-list.html

[34] "Cyber Crime Warnings for India," *BBC*, May 6, 2012, http://www.bbc.com/news/business-17979980

[35] See Cyber Crime in Turkey www.spk.gov.tr/displayfile.aspx, slides 20-41

[36] Peter Chalk, *The Maritime Dimension of International Security: Terrorism, Piracy, and Challenges for the United States*, (Rand: Santa Monica, 2008), http://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG697.pdf

[37] Ryan Sherstobitoff , "Dissecting Operation Troy: Cyberespionage in South Korea," *McAfee*, 2013, http://www.mcafee.com/us/resources/white-papers/wp-dissecting-operation-troy.pdf

[38] Ponemon Institute, "Cost of Cyber Crime Study 2013: The United States," October 2013: http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf: 16; "Reputational Risk And IT: How Security And Business Continuity Can Shape the Reputation and Value of Your Company," *2012 IBM Global Reputational Risk and IT Study*, September 2012, http://www-935.ibm.com/services/us/gbs/bus/html/risk_study.html

[39] "The World's Community and the War on Cyber Crime—What About Italy?" slide 12, https://www.securitysummit.it/upload/file/Atti/22.03.12_JART%20ARMIN.pdf

[40] "Keeping the UK safe in cyber space," March 14, 2014, https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace

[41] "Target Hackers Broke in Via HVAC Company," Krebs on Security, February 14, 2014, http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

[42] Lawrence A. Gordona, Martin P. Loeba, and Lei Zhoua, "The impact of information security breaches: has there been a downward shift in costs?" *Journal of Computer Security*, Vol. 19, 2011 http://iospress.metapress.com/content/n3054376432h7358/fulltext.pdf: 33-56

[43] Economist of the Brazilian Institute of Economics/Getulio Vargas Foundation (IBRE/FGV)

[44] Data about GDP and population: World Economic Outlook of the International Monetary Fund (WEO/IMF), http://www.imf.org/external/pubs/ft/weo/2013/02/weodata/index.aspx

[45] http://saladeimprensa.ibge.gov.br/en/noticias?view=noticia&id=1&idnoticia=2575&busca=1&t=desocupacao-foi-4-3-dezembro-fecha-2013-media-5-4

[46] http://www.bcb.gov.br/pec/appron/apres/CarlosHamilton_CAE_09-11-20112.pdf

[47] http://www.internetworldstats.com/stats2.htm

[48] http://www.internetworldstats.com/stats.htm

[49] http://www.pwc.com.br/pt/publicacoes/assets/pesquisa-crimes-digitais-11-ingles.pdf

[50] Exchange rate of R $ / U.S. $ 2.37 (average of 2014, until 03/25/14)

[51] http://www.ciab.com.br/_pdfs/publicacoes/2012/43-Dez2012.pdf

[52] http://www.pwc.com.br/pt/publicacoes/assets/pesquisa-crimes-digitais-11-ingles.pdf

[53] Source: IMF

[54] Davidson, James Dale. *Brazil is the New America: How Brazil Offers Upward Mobility in a Collapsing World*, 2012, http://books.google.com.ph/books?id=8muXHC8xQBIC&pg=PT125&img=1&zoom=3&hl=en&ots=yf3cfKKtQR&sig=ACfU3U1214BNCrmKbjl6ora5b4ccYOF1Ow&w=685

[55] http://www.nytimes.com/2003/10/27/business/technology-brazil-becomes-a-cybercrime-lab.html?src=pm

[56] http://www.forbes.com/sites/ricardogeromel/2012/03/02/hackers-stole-1billion-in-brazil-the-worst-prepared-nation-to-adopt-cloud-technology/

[57] http://g1.globo.com/politica/noticia/2014/03/governo-e-camara-dizem-que-marco-da-internet-sera-votado-nesta-terca.html

McAfee
An Intel Company

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

61079rpt_csis-econ-cybercrime_0614_ETMG