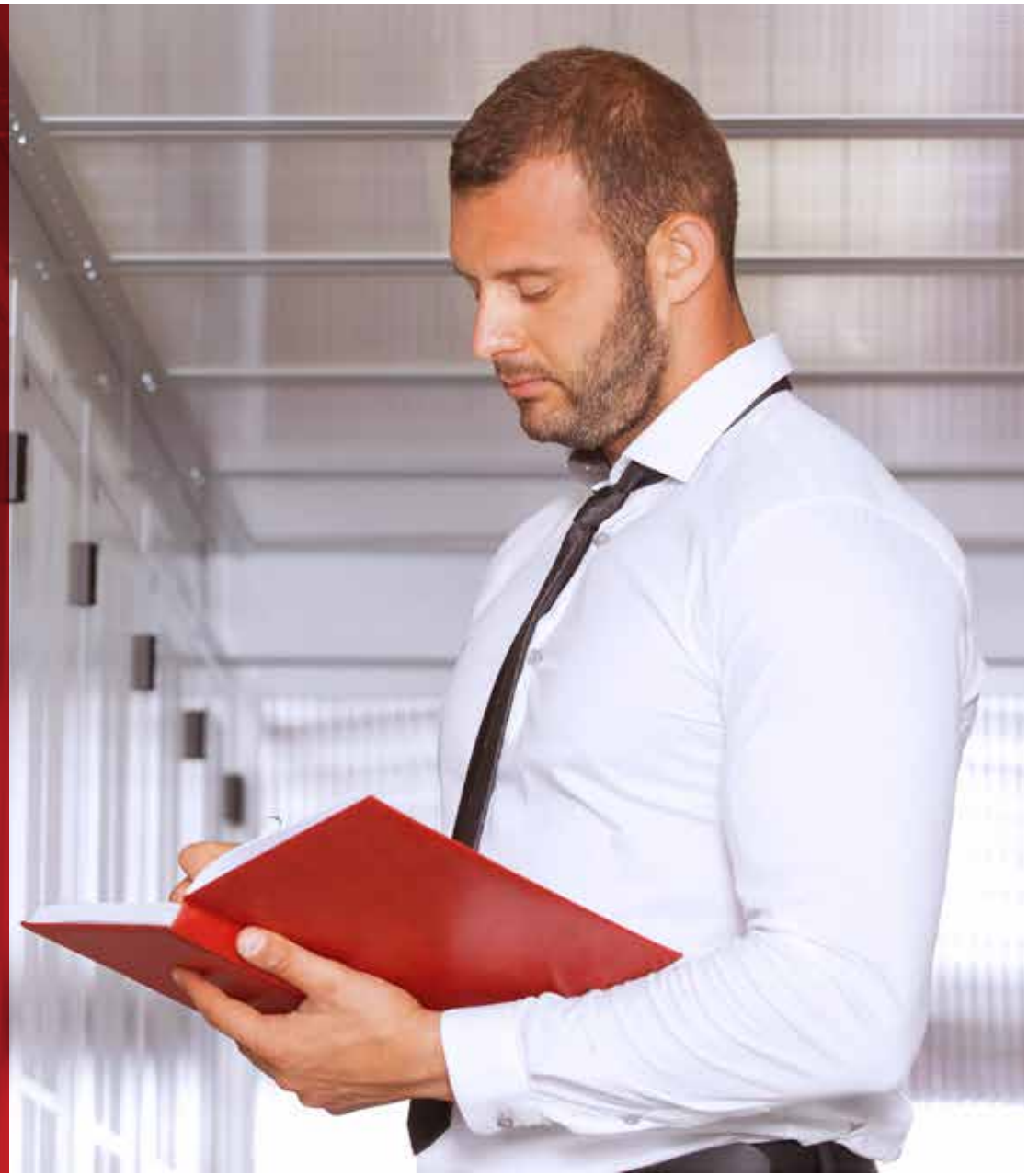
REPORT

McAfee
Together is power.

Economic Impact of Cybercrime—No Slowing Down

February 2018



CSIS

Table of Contents

Authors

This report was researched and written by:

- **James Lewis**

Economic Impact of Cybercrime—No Slowing Down

Cybercrime Overview

Cybercrime is relentless, undiminished, and unlikely to stop. It is just too easy and too rewarding, and the chances of being caught and punished are perceived as being too low. Cybercriminals at the high end are as technologically sophisticated as the most advanced information technology (IT) companies, and, like them, have moved quickly to adopt cloud computing, artificial intelligence, Software-as-a-Service, and encryption. Cybercrime remains far too easy, since many technology users fail to take the most basic protective measures, and many technology products lack adequate defenses,[1] while cybercriminals use both simple and advanced technology to identify targets, automate software creation and delivery, and monetization of what they steal.

This is the third report on the cost of cybercrime that CSIS has done with McAfee ("The Economic Impact of Cybercrime," 2013, and "Net Losses," 2014). In those reports, we set upper and lower bounds for cybercrime by comparing it to similar kinds of crime. We found that the difficulty of monetizing cybercrime, particularly for IP theft, can skew estimates—criminals did not always gain the full value of what they had stolen (a conclusion based in part on two roundtables we held with economists and lawyers). For the 2014 report, we surveyed publicly available information on national losses, finding data on roughly 50 countries. In a few cases, we used not-for-attribution interviews with cybersecurity officials (including all G7 countries) on their estimates of loss. Combined with the work of the 2013 report/study, this enables us to develop an estimate of the range of potential cybercrime loss as a percent of national gross domestic product (GDP). We compared this estimate with the reported loss for the handful of countries where we had more confidence in national data collection and reporting.

As illegal activities go, cybercrime is not the most expensive. That honor goes to government corruption, followed by narcotics trafficking, with its accompanying fatalities. Cybercrime ranks third in dollar value as a global scourge.[2]

Where cybercrime is the undisputed leader, however, is in its ability to make hundreds of millions of people victims. A good estimate is that two-thirds of the people online—more than two billion individuals—have had their personal information stolen or compromised. One survey found that 64% of Americans had been victims of fraudulent charges or loss of personal information. Cybercrime is front-page news because it touches everyone.[3]

Cybercrime also leads in the risk-to-payoff ratio. It is a low risk crime that provides high payoffs. A smart cybercriminal can make hundreds of thousands, even millions of dollars with almost no chance of arrest or jail.[4] When you think of big cybercrimes, from Target to SWIFT to Equifax, none of the perpetrators have been prosecuted to date. Law enforcement agencies can be aggressive and skillful in pursuing cybercriminals, but many operate outside their reach. This is one reason why the cost of cybercrime continues to grow.

In 2014, CSIS estimated that cybercrime costs the world's economy almost $500 billion, or about 0.7% of global income. That is more than the income of all but a handful of countries, making cybercrime a very lucrative occupation. Our current estimate is that cybercrime may now cost the world almost $600 billion, or 0.8% of global GDP. The reasons for this growth are as follows:

- Quick adoption of new technologies by cybercriminals
- The increased number of new users online (these tend to be from low-income countries with weak cybersecurity)
- The increased ease of committing cybercrime, with the growth of Cybercrime-as-a-Service
- An expanding number of cybercrime "centers" that now include Brazil, India, North Korea, and Vietnam
- A growing financial sophistication among top-tier cybercriminals that, among other things, makes monetization easier.

Monetization of stolen data, which has always been a problem for cybercriminals, seems to have become less difficult because of improvements in cybercrime black markets and the use of digital currencies. Stolen credit card numbers and personally identifiable information (PII) are offered for sale in quantity on the dark web using a complex set of transactions involving brokers and other intermediaries in black markets. Financial theft is transferred to the criminals' own bank accounts through a series of transfers intended to disguise and confuse. Intellectual property is either used by the acquirers or sold. Digital currency makes ransomware payments easier and less traceable. The increased ease of monetization is another reason why cybercrime has increased.

Cybercrime operates at scale. The amount of malicious activity on the internet is staggering. One major internet service provider (ISP) reports that it sees 80 billion malicious scans a day, the result of automated efforts by cybercriminals to identify vulnerable targets. Many researchers track the quantity of new malware released, with estimates ranging from 300,000 to a million viruses and other malicious software products created every day.[5] Most of these are automated scripts that search the web for vulnerable devices and networks. Phishing remains the most popular and easiest way to commit cybercrime, with the Anti-Phishing Working Group

Monetization of stolen data, which has always been a problem for cybercriminals, seems to have become less difficult because of improvements in cybercrime black markets and the use of digital currencies.

(APWG) recording more than 1.2 million attacks in 2016, many linked to ransomware.[6] This number may be low, since the FBI estimated there were 4,000 ransomware attacks every day in 2016. The Privacy Rights Clearing House estimates there were 4.8 billion records lost as a result of data breaches in 2016, with hacking responsible for about 60% of these.

Cybercrime	Estimated Daily Activity
Malicious scans	80 billion
New malware	300,000
Phishing	33,000
Ransomware	4,000
Records lost to hacking	780,000

Table 1. Estimated daily cybercrime activity

New technologies make people and companies more efficient and effective, cybercriminals included. Cybercriminals adopt new technologies at a fast pace. Malware writing is automated, with thousands of new pieces generated every day. TOR, a free software product that enables anonymous and untraceable internet activity, has become a preferred avenue for cybercriminals, who prefer operating in the "Dark Web." As internet activity has moved to mobile platforms, cybercrime has followed. Some cybercriminals even use artificial intelligence tools to find targets. Finally, Bitcoin and other digital currencies are both targets for theft and a means of payment and money transfers for cybercriminals. North Korea, for example, made hacking South Korean Bitcoin exchanges—before Bitcoin was banned—an art form.[7] Other countries' Bitcoin exchanges may have been targeted, and the increase in value of digital currencies makes them desirable targets.

Combine anonymizing services and anonymized digital currencies with already sophisticated cybercrime black markets—sophisticated in the way they are organized, in their specialization, and in the attack tools they offer, often designed to evade network defenses—and you solve one of the major problems cybercriminals faced in the past: how to monetize the information they had stolen. The mixture of anonymizing services like the "Tor" network, digital currencies, and the dark web, creates a parallel universe that gives cybercriminals both an arsenal and a sanctuary.[8]

We expect further growth in cybercrime as hackers take advantage of poorly protected "internet of things" (IoT) devices that, while themselves not particularly valuable, provide new, easy approaches to steal personal information or gain access to valuable data or networks. IoT devices also allow, as we have seen, for massive denial-of-service (DoS) attacks that block services and impose costs on companies and individuals. Cybercrime will also continue to grow as hackers increase their use of artificial intelligence tools to create malware and identify targets and move into the cloud. Criminals will take advantage of cloud services both as targets and as tools to house malware and launch DoS attacks.

North Korea, for example, made hacking South Korean Bitcoin exchanges—before Bitcoin was banned—an art form.[7]

The Global Cost

Criminal activity on the internet is much broader that cybercrime as essentially all elements of human criminal activity have moved into cyberspace. A senior British official reported, for example, that half of all reported crime in the UK is cyber-related. We did not attempt to measure the cost of all malicious activity on the internet and focused instead on a narrower definition based on criminals gaining illicit access to a victim's computer or network. Using this definition, the elements of cybercrime cost we have identified include:

- The loss of intellectual property and business confidential information
- Online fraud and financial crimes, often the result of stolen personally identifiable information (PII)
- Financial manipulation, using stolen sensitive business information on potential mergers or advance knowledge of performance reports for publicly traded companies
- Opportunity costs, including disruption in production or services, and reduced trust for online activities. This includes the effect of ransomware, which involves both payments to redeem encrypted data, and, more importantly, serious disruptions to services and output.
- The cost of securing networks, buying cyberinsurance, and paying for recovery from cyberattacks
- Reputational damage and liability risk for the hacked company and its brand, including temporary damage to stock value

Estimates of the cost of cybercrime still show significant variation, from tens of billions to a trillion dollars or more. This reflects the absence of data and differing methodologies. We borrowed modeling techniques from economic history research, where data is usually incomplete and discontinuous, in an effort to model the cost of cybercrime. This modeling effort estimates that the global cost of cybercrime may be as much as $600 billion according to CSIS estimates.

This is a significant increase from three years ago. CSIS believes that five trends help explain this. The first is state-sponsored bank robbery, followed by ransomware, Cybercrime-as-a-Service, an increased reliance on anonymization services (such as Tor and digital currencies), and, finally, the prevalence of the theft of personal information and the theft of intellectual property (IP).

In 2014, taking into account the full range of costs, CSIS estimated that cybercrime cost the world between $345 billion and $445 billion.[9] As a percentage of global GDP, cybercrime cost the global economy 0.62% of GDP in 2014. Using the same methods, CSIS now believe the range is now between $445 billion and $600 billion. Our second effort at a global estimate suggests that as a percentage of global GDP, cybercrime cost the global economy 0.8% in 2016.[10] Our estimate tried to account for underreporting of losses by companies and governments by extrapolating from the loss rate for countries where we found credible data—these countries accounted for roughly two-thirds of global GDP.

This modeling effort estimates that the global cost of cybercrime may be as much as $600 billion according to CSIS estimates.

Region (World Bank)	Region GDP (USD, trillions)	Cybercrime Cost (USD, billions)	Cybercrime Loss (% GDP)
North America	20.2	140 to 175	0.69 to 0.87%
Europe and Central Asia	20.3	160 to 180	0.79 to 0.89%
East Asia & the Pacific	22.5	120 to 200	0.53 to 0.89%
South Asia	2.9	7 to 15	0.24 to 0.52%
Latin America and the Caribbean	5.3	15 to 30	0.28 to 0.57%
Sub-Saharan Africa	1.5	1 to 3	0.07 to 0.20%
MENA	3.1	2 to 5	0.06 to 0.16%
World	**$75.8**	**$445 to $608**	**0.59 to 0.80%**

Table 2. Regional Distribution of Cybercrime 2017

CSIS compared the level of loss to the cybersecurity maturity level. The Global Cybersecurity Index (GCI)[11] is an initiative by the ITU to measure the commitment of countries to cybersecurity across industries and sectors. Each country's level of cybersecurity development is measured in five categories: legal measures, technical measures, organizational measures, capacity building, and cooperation. We divided the survey results into three categories: countries whose economies are digitized and have mature cybersecurity capabilities; countries who are increasingly digitized but are still developing their cybersecurity capabilities; and countries whose economies are only beginning to be digitized and where cybersecurity efforts are just beginning.

	GCI Score	% GDP to Low	% GDP to High	% GDP to Average	% GDP (excluding outliers)
Leading	0.7+	0.014%	1.35%	0.37%	0.411%
Maturing	0.3-0.7	0.000096%	1.83%	0.41%	0.513%
Initiating	0-0.3	0.024%	0.29%	0.11%	0.117%

Table 3. Cybercrime by Level of Maturity (Global Cybersecurity Index)

The cost of cybercrime is unevenly distributed among all the countries of the world. CSIS found variations by region, income levels and level of cybersecurity maturity. Unsurprisingly, the richer the country, the greater its loss to cybercrime is likely to be. The relationship of the developing world to cybercrime is complex, as the mobile connections that have brought the internet to millions are easily exploitable, but the value that can be extracted from these connections remains relatively low, and weak defenses in wealthier countries mean that is where criminals focus their attention. The countries with the greatest losses (as a percentage of national income) are in the mid-tier nations—those that are digitized but not yet fully capable in cybersecurity.

	GNI/ capita range	% GDP	% GDP to High	Average	% GDP (excluding outliers)
High	> $12,236	0.014%	1.83%	0.45%	0.505%
Upper-Middle	$3,956 to $12,235	0.014%	1.345%	0.412%	0.449%
Lower-Middle	$1,006 to $3,955	0.000096%	0.25%	0.10%	0.143%
Low	< $1,005	0.035%	0.035%	0.035%	0.035%

Table 4. World Bank Income Group Brackets

Estimation Issues

Any estimate of the cost of cybercrime faces several problems. The first is underreporting by victims and the paucity of data collection by governments, a problem that is compounded in some countries by reporting regulations that differ among industry sectors. The UK, for example, estimates, that only 13% of cybercrime are reported.[12] Most governments can tell you the number of car thefts or even thefts of postage stamps, but not online crime. A failure to collect data is compounded by reluctance on the part of many companies to report when they have been victims. Data collection remains a problem, and national estimates are still remarkably imprecise. The most significant limitation in developing an estimate of the cost of cybercrime is underreporting. Only a fraction of losses are reported, as companies seek to avoid liability risks and reputational damage.

Second, the cost of online risk-avoidance, where people choose to go back to paper or avoid online transactions because of their fears of cybercrime, is difficult to estimate. Generally, the attractiveness of digital technologies is still too compelling for people and companies to give up the internet, but there are signs of incipient change.

Third, one big problem with our estimated cost is that it provides the aggregate cost to countries, not individual companies or consumers, and doesn't accurately reflect a skewed distribution when it comes to victims. For example, if a country had 10 companies and lost $100 a year to cybercrime, the average cost per company is $10. In fact, the real distribution is that two companies lose $50 and the other eight lose little or nothing. A national aggregate conceals the fact that losses are unevenly distributed among companies and some companies may remain unaware of cybercrime losses.

To give us upper and lower boundaries for the cost of cybercrime, essentially a way to see if our estimates were reasonable, we again looked at other crimes where costs have also been quantified, to help us scope the cost of malicious cyberactivity. Crime is a "normal" part of social interaction and international affairs, and governments individually and cooperatively take steps to manage and reduce the cost of crime. Our assumption is that cybercrime mirrors other criminal activities.

- **Maritime piracy:** One estimate puts the annual cost of piracy as somewhere between $5.7 and $6.1 billion in 2012 and, for West and East Africa together, $4.2 billion in 2016.[13]
- **Pilferage:** Companies accept "pilferage" as part of the cost of doing business. Using pilferage rates as an analogy, the cost of cybercrime in the US is between 0.5% and 2% of national income.
- **Transnational crime:** The UN Office on Drugs and Crime estimated the cost of all transnational organized crime as $870 billion in 2012, or 1.2% of global GDP.[14] Six hundred billion dollars of this came from illegal drug trafficking.
- The World Economic Forum (using 2011 data) estimated the total cost of global crime at $1.8 trillion, or about 1.5% of global GDP.[15] The research

organization Global Financial Integrity estimated that all transnational crime cost the world $1.6 trillion to $2.2 trillion in 2017.[16] Cybercrime would make up about one seventh of these costs.

Data on cybercrime remains poor because of underreporting and a surprising laxness in most government efforts around the world to collect data on cybercrime. This may change as the cyberinsurance market continues to grow and as insurance companies develop policies and collect actuarial data to estimate risk, but this process will likely take years to complete. The National Association of Insurance Commissioners estimated that $1 billion in cybersecurity insurance was sold in 2016 in the US, a fraction of what the hundreds of billions spent on fire or maritime insurance.

The cost to the individual victim can be low, with few exceptions. Many consumers, while worried, shrug off the risk. Victim companies can suffer dramatically and embarrassingly, but, to our surprise, many big companies see the financial loss from hacking as the cost of doing business online. The Poneman Institute estimates that the average cost of a breach is $3.6 million dollars, which is painful but not crippling for big companies. The real risk lies in damage to brand and increased liability risk. Big companies in particular "self-insure," gambling that any loss will be manageable. Perhaps this kind of tolerance, combined with underreporting, is one reason why cybercrime remains so pervasive._

Financial Cybercrime

Banks remain the favorite target of skilled cybercriminals. This has been true for more than a decade. Cybercrime imposes a heavy cost on financial institutions as they struggle to combat fraud and outright theft. One report says that banks spend three times as much on cybersecurity as non-financial institutions,[17] and there is agreement among bank regulators around the work that cybercrime poses a "systematic" risk to financial stability. To understand why financial cybercrime is such a problem, we need to look at three countries in particular.

The combination of massive budgets, access to talent, and protection from law enforcement make nation-states the most dangerous source of cybercrime. CSIS believes that three countries—Russia, North Korea, and Iran—are the most active in hacking financial institutions. China remains the most active in espionage. Iran's goals are coercive effect, as evidenced by the Iranian distributed denial-of-service (DDoS) attack on leading US banks).[18]

CSIS believes that for cybercrime, the two most important states are Russia and North Korea. They hack banks to make money. A former NSA Deputy Director said publicly in March, that "nation states are robbing banks," and they're doing it with computers.[19] He was referring to the 2015 to 2016 cybercrime campaign that targeted dozens of banks in the SWIFT network. Tens of millions of dollars were stolen from banks in developing countries

In 2016, the SEC's online database for financial filings was breached, and attackers were able to access nonpublic information. The SEC publicly acknowledged[1] the hack in September 2017, saying that hackers may have used the information to make profitable trades.

by submitting fake payment orders via the network.[20] Security researchers linked the attacks to the North Korean Reconnaissance General Bureau (RGB).[21] The attacks provided a lucrative means to supplement the North Korean government's limited access to foreign currency.

North Korea has also turned to cryptocurrency theft to help fund its regime.North Korean hackers have targeted at least three South Korean cryptocurrency exchanges in 2017.[22] Cryptocurrencies are a particularly valuable target for North Korea, who are able to use Bitcoin's anonymity to circumvent international sanctions. Some researchers have speculated that North Korean actors have also been involved in attempts to surreptitiously install Bitcoin mining software on hacked computers, hijacking networks of compromised systems to mine for cryptocurrencies.[23] The Pyongyang University of Science and Technology has begun offering its computer science students classes in Bitcoin and Blockchain, confirming the growing interest in cryptocurrencies for North Korea.[24]

As major international financial institutions invest in defense, better fraud prevention, and transaction authentication, the most sophisticated nation-states and organized crime groups have begun targeting the "seams" between well-defended networks, exploiting weak points in the global financial network to pull off massive heists. The North Korean campaign to steal money through the SWIFT network is a prime example. Recognizing the difficulty of pulling off large-scale thefts from a single major western bank, the RGB targeted smaller, less sophisticated banks in developing countries like Bangladesh, Vietnam, and Ecuador.[25] After compromising these banks' systems, they then used the victim banks' credentials to send what looked like legitimate SWIFT fund transfer requests to larger banks in other countries.[26] These requests at first appeared legitimate to the receiving banks, since they were sent from legitimate partner banks through the established channels, so in some cases the money was transferred.

CSIS believes that Russia leads overall in cybercrime, reflecting the skill of its hacker community and its disdain for western law enforcement. The complex and close relationship between the Russian state and Russian organized crime means that Russia provides a sanctuary for the most advanced cybercriminals, whose attention focuses on the financial sector.[27] The best cybercriminals in the world live in Russia, and, as long as they do not travel to countries where they could be arrested, they are largely immune from prosecution. For example, one of the cybercriminals who hacked Yahoo at the behest of Russian intelligence services, compromising millions of accounts and transferred the PII to the Russian government, also used the stolen data for spam and credit card fraud for personal benefit.[28]

Hackers in these countries, whether affiliated with the state or not, account for much of the cybercrime that occurs in the world. Until these nation-states change their behavior, either by stopping state support for hacking or by enforcing laws against criminal hackers, cybercrime will remain a major international problem.

In 2011, North Korean hackers used software to accumulate gaming points on a number of popular South Korean gaming sites. The points were then exchanged online for cash. South Korea's International Crime Investigation Unit said the hackers accumulated $6 million in less than two years. They were expected to send at least $500 per month back to the North Korean government for a slush fund that is used in part to fund North Korea's nuclear program.

Ransomware

Ransomware is the fastest growing cybercrime. Ransomware victims include big companies, small and medium enterprises, and individual consumers. While the cost to the individual is low, usually about $200 in ransom, the ability to hit thousands of targets at a low cost and with no risk of penalty explains why this category of cybercrime is growing so quickly. While many victims do not pay ransom, enough do to make this profitable. The FBI reported $209 million in ransom was paid in the first quarter of 2016, compared to just $24 million in ransom payments in all of 2015.[29] What prompted such explosive growth?[30]

Ransomware began years ago with floppy disks sent through the mail, inviting victims to take a survey assessing their risk of contracting AIDS. When the disk was inserted, its software locked their computers and demanded $189 in cash be sent to a P.O. box in Panama.[31] It has since become much more sophisticated.[32] Ransomware has gone from artisanal exploit to mass-market. Until 2015, ransomware campaigns were typically run by organized crime groups that wrote their own code.[33] From 2012 to 2015, 33 new ransomware offerings were released, but that number doubled in 2016, with 70 new families of ransomware products made available.[34]

We are seeing the commercialization of ransomware, with turnkey ransomware toolkits available online for a few dollars and as much as $3,000 for specialized offerings. The median cost of buying a ransomware package is only $10, allowing many hackers to carry out ransom attacks. Currently, more than 6,000 online criminal marketplaces sell ransomware products and services, offering more than 45,000 different products.[35]

As quickly as ransomware kits gained popularity, however, they began to be replaced by Ransomware-as-a-Service (RaaS). RaaS allows for the authors of ransomware programs to vastly extend their potential reach by opening their code for use by almost any other cybercriminal. Instead of a single actor or group writing ransomware and distributing it themselves, the RaaS model allows for authors to set up platforms where "affiliates" can deploy it to their own list of targets.[36] Typically, the authors take a cut of the resulting ransoms, though some may charge an up-front fee or sell blocks of time to access the command and control servers running the campaign.[37] Email is still by far the most popular means of compromising target computers, meaning that with access to darknet RaaS offerings, anyone with the ability to successfully phish a target can begin to profit from ransomware.[38] This ease of use has been the main driver of ransomware's growth, and, as long as victims continue to pay, cybercriminals will continue to flock to ransomware offerings.

One emerging trend is ransomware worms, which work their way through networks to lock out many more computers than just the initial target. The WannaCry incident showed how these worms work, and it is likely that we will see more attacks like this. New ransomware attacks are expected to gain exfiltration capabilities, stealing target files and locking the user out at the same time.[39] Finally, ransomware is expected to increasingly target mobile systems, with Android ransomware kits already beginning to appear on marketplaces as

Currently, more than 6,000 online criminal marketplaces sell ransomware products and services, offering more than 45,000 different products.[35]

cybercriminals look to take advantage of the massive number of unsecured phones worldwide.[40] IoT devices are also expected to be more frequently targeted due to their lack of security protections, with industrial IoT, in particular, offering a potentially juicy target to bad actors.[41]

Cybercrime-as-a-Service (CaaS)

Over the last 20 years, we have seen cybercrime become professionalized and sophisticated. Cybercrime is a business with flourishing markets offering a range of tools and services for the criminally inclined.[42] From products like exploit kits and custom malware to services like botnet rentals and ransomware distribution, the diversity and volume of cybercrime offerings has never been greater. The result of this has been a simultaneous broadening and deepening of the cybercrime threat. New tools and platforms are more accessible than ever before to those without advanced technical skills, enabling a flood of new actors to engage in cybercrime activities.[43] At the same time, experienced criminals are able to focus on developing more specialized skill sets, confident in their ability to find others within the thriving darknet ecosystem who can complement their services, and with whom they could collaborate to develop new tools of unprecedented sophistication.[44]

The cybercrime ecosystem has undergone an evolution as it has grown in sophistication to accommodate arrival of new actors, and new scrutiny. The threat of law enforcement action has forced most cybercrime dealings onto the dark web, where the anonymity of Tor and Bitcoin protects actors from easy identification. Trust is difficult to come by in these communities, leading some markets to implement systems of escrow payment to facilitate high-risk transactions and prompting some sellers to offer support services and money-back guarantees on their wares.[45] The markets have also become stratified, as expert criminals increasingly isolate themselves within highly selective discussion boards to limit the threat from police and fraudsters.[46] Despite this, a thriving cybercrime economy has emerged from these communities, offering everything from product development to technical support, distribution, quality assurance, and even help desks.[47]

Cybercriminals have become reliant on the Tor network to maintain anonymity. Tor, short for The Onion Router, allows users to browse the internet anonymously by encrypting their traffic and then routing it through multiple random relays on its way to its destination. This process makes it nearly impossible for law enforcement agencies to track users or determine the identities of visitors to certain sites. While Tor can be used to anonymously browse ordinary sites like Wikipedia or YouTube, its greatest advantage to cybercriminals comes in its ability to access special "dot.onion" addresses on the dark web, which serves as the home for most internet black markets.

As of June 2017, Europol found that the Tor network had more than 2.2 million users and hosted almost 60,000 unique onion domains. Researchers disagree over how much of the traffic on Tor is illicit, but one recent study has estimated that approximately 57% of onion sites hosted illegal content.[48] Though some law enforcement actions have managed to exploit vulnerabilities in Tor to take down sites hosting child pornography, Tor is still considered to be highly resilient to law enforcement

According to the FBI, DDoS-for-hire are advertised in criminal forums and available on dark web marketplaces. They offer criminals the ability to anonymously attack any internet target.

efforts. Most of the successes in shutting down dark net marketplaces in the past were the result of police exploiting mistakes made by site administrators, not through the compromise of Tor itself.

While the number of participants in these communities is massive—the FBI estimated that marketplace AlphaBay had serviced over 200,000 users and had 40,000 vendors before its takedown in July 2017[49]—some law enforcement officials have estimated that a much smaller number of individuals may be responsible for the bulk of the most significant cybercrime offerings. In 2015, the deputy director of the UK National Cybercrime Unit stated that law enforcement believed that much of the CaaS economy was built on the work of only 100 to 200 people.[50] These individuals often profit handsomely from their involvement. One research group found that some criminals can make more than $100,000 a year just selling ransomware kits, more than twice the annual salary of a software developer in Eastern Europe, where many of these criminals operate.[51]

There are numerous ways for a cybercriminal to profit without ever having to engage in the "traditional" cybercrime acts like financial fraud or identity theft. The first is Research-as-a-Service,[52] where individuals work to provide the "raw materials" for future criminal activities. This can include selling knowledge of system vulnerabilities to malware developers, or auctioning off lists of email addresses to spammers. The sale of software exploits has gained significant attention recently, as groups like the Shadow Brokers have announced controversial subscription programs giving customers access to unpatched system vulnerabilities.[53]

The number of discovered zero-day exploits—those that had been previously undetected by the product's vendor—has steadily decreased since 2014, most likely the result of the growth of "bug bounty" programs that incentivize the legal disclosure of vulnerabilities.[54] This reduction has led to an increase in price for the vulnerabilities that do get discovered, with some of the most valuable being sold for more than $100,000 in one of the many dark net marketplaces catering to exploit sales.[55] Other cybercrime actors may specialize in selling email databases to facilitate future cybercrime campaigns, such as in the case of the recent sale of three billion Yahoo accounts to several spammers for $300,000 each.[56]

One major domain of malware development are web injections—pieces of code that allow hackers to gain control of a target website and modify the web pages to trick victims into giving up sensitive information. Web injection is one of the most likely stages in malware development to be outsourced by major cybercriminal groups due to the specialization involved.[57]

Exploit kits are another popular product on darknet marketplaces, offering novice cybercriminals the tools to break into a wide range of systems. However, work by Europol suggests that the popularity of exploit kits has fallen off over the past year as top offerings have been shut down and replacements have struggled to maintain the same level of sophistication or popularity.[58] Europol also noted that theft through malware was generally becoming less of a threat as cybercriminals increasingly turn to tools like ransomware and DDoS extortion, which are easier to monetize.

One major domain of malware development are web injections—pieces of code that allow hackers to gain control of a target website and modify the web pages to trick victims into giving up sensitive information. Web injection is one of the most likely stages in malware development to be outsourced by major cybercriminal groups due to the specialization involved.[57]

The third way hackers can profit from the growing sophistication of the cybercrime economy is by providing cybercrime Infrastructure-as-a-Service. Actors involved in this field are responsible for providing the services and infrastructure other criminals rely on to execute their attacks. Examples of infrastructure services include bulletproof hosting and botnet rentals. Bulletproof hosting helps cybercriminals establish web pages and servers on the internet without threat of law enforcement takedowns. Botnet rentals allow cybercriminals to pay for temporary access to a network of infected computers, using them for anything from spam distribution to DoS attacks.

The use of botnets for DoS attacks has proven to be a particularly profitable endeavor for many cybercriminals who extort money from website owners by threatening an attack that would overwhelm and shut down their services. Researchers have estimated that a botnet costing only $60 a day can inflict as much as $720,000 in damages on victim organizations,[59] and the hackers controlling the botnets enjoy a profit margin of more than 70% when renting their services out to other criminals.[60] The use of botnets will likely grow in the coming years as cybercriminals continue to exploit vulnerabilities in IoT devices to create even larger networks.[61] The danger presented by IoT botnets was clearly demonstrated in 2016, when the massive Mirai IoT botnet attacked domain name provider Dyn, bringing down sites like Twitter, Netflix, Reddit, and CNN in the largest attack of its kind ever seen.[62]

Tor and Bitcoin

CSIS sees the expansion of cybercrime has been enabled by the easy availability of tools like Bitcoin and Tor, which have allowed cybercriminals to conceal their identities while paying for services through a digital medium that significantly complicates law enforcement tracking efforts. Bitcoin has long been the favored currency for darknet marketplaces, with cybercriminals taking advantage of its pseudonymous nature and decentralized organization to conduct illicit transactions, demand payments from victims, and launder the proceeds from their crimes.[63] Cybercriminals benefit from the fact that no personally identifying information is linked to the use and exchange of Bitcoin, allowing criminals to operate with near impunity despite the fact that all Bitcoin transactions are publicly recorded.

Bitcoin users can only be identified if their accounts become linked to their real identity, something most criminals are careful to avoid. However, linking an account with identifying information is a necessary component of converting Bitcoin into real-world currencies through banks or exchanges, creating a vulnerability for criminals. To address this, a number of services have been established in recent years that allow cybercriminals to launder their Bitcoins and withdraw them through unregulated exchanges to avoid being caught. Bitcoin laundering can occur through the process of "tumbling," or "mixing," where multiple users pool both clean and dirty Bitcoins together, letting a program execute a series of exchanges between the members that eventually gives the users back their money in randomized coins.[64] Cybercriminals can also

Bitcoin laundering can occur through the process of "tumbling," or "mixing," where multiple users pool both clean and dirty Bitcoins together, letting a program execute a series of exchanges between the members that eventually gives the users back their money in randomized coins.[64]

utilize unregulated cryptocurrency exchanges that obscure customer information, like in the case of the recently shut down BTC-e exchange, thought to be responsible for 95% of all ransomware cash outs.[65]

Despite these services, there are still instances in which cybercriminal using Bitcoins can be identified, either through IP address mapping[66] or accidental leaks by web trackers.[67] As a result, a number of attempts have been made at developing a truly anonymous cryptocurrency that could provide greater security to cybercriminals. The three most popular today are Dash, Monero, and Zcash. Dash uses a technique known as "coinjoin" to integrate mixing into the operation of the currency and to provide protection for senders and recipients. Monero is even more secure, using "stealth addresses" that hide the amount of every purchase and mix each transaction with more than a hundred others to anonymize the senders.[68] Zcash, the most advanced of the three, using a process called zero-knowledge proofs to allow two users to exchange information without ever revealing identities, completely shielding details of the transaction from all involved.[69] Monero has been the most widely implemented of the three, with about 2% of all transactions on former top market AlphaBay using the coin in late 2016.[70] According to Europol, a Monero-based ransomware kit has already appeared in the wild this year, raising the possibility that cybercriminals may soon begin to use these anonymous cryptocurrencies for more than just exchanging services in darknet markets.[71]

Cybercriminals are looking for even better security by using an emerging new marketplace, OpenBazaar. OpenBazaar is a decentralized, peer-to-peer network that allows users to make purchases without ever hosting data on a central server.[72] This would make the market extremely difficult to disrupt, as law enforcement have already found with similar peer-to-peer networks like BitTorrent. Though little illegal activity has so far occurred on OpenBazaar that might change once Tor is fully implemented and anonymous cryptocurrencies like Monero are integrated into the platform. In their 2017 Internet Organised Crime Threat Assessment, Europol highlighted OpenBazaar as a potential future threat.[73]

Intellectual Property Theft

The most important area for the cost of cybercrime is in the theft of intellectual property and business confidential information. Internet connectivity has opened a vast terrain for cybercrime, and IP theft goes well beyond traditional areas of interest to governments, such as military technologies. One way to measure the cost of intellectual property theft is to look for competing products that take market share from the rightful owners. If hackers steal intellectual property, such as product designs, from a small or medium-size enterprise, it can be a fatal experience. For big companies, it can be an unexpected source of revenue lost as competing products enter the market. The theft of intellectual property accounts for at least a quarter of the cost of cybercrime and, when it involves military technology, creates risks to national security as well. These losses can often be invisible to the victim. They still have access to the IP that has been copied by the criminals and may attribute a decline in revenue to growing competition rather than theft.

The theft of intellectual property accounts for at least a quarter of the cost of cybercrime and, when it involves military technology, creates risks to national security as well.

China is the focus of IP theft concerns. There is a general consensus that Chinese hackers, often associated with the People's Liberation Army (PLA,) led until recently in the theft of intellectual property.[74] Before 2015, China was responsible for half of the cyberespionage against the US involving the theft of IP and commercially valuable information, according to US government sources. This probably caused $20 billion in harm annually (the rest of the total cost to the US of cybercrime came from financial crime, recovery costs and extra company spending on defenses, accounting for perhaps $100 billion in 2014, according to US officials. While the evidence is mixed, a review of publicly known cases suggest the three quarters of Chinese espionage was for commercial purposes, suggesting the 2015 Obama Xi agreement on commercial cyberespionage may have "saved" the US perhaps as much as $15 billion a year.

At the 2015 Xi-Obama Summit, both leaders agreed that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors." Although opinions on compliance with the agreement are mixed, until recently, China appears to be living up to its commitments under the agreement. The language of this agreement was drafted by the US to allow continued espionage. It is not an agreement to end cyberespionage. The US insisted on this language, not only to reduce state-sponsored Chinese commercial espionage but also to ensure that spying per se is not ruled out. It is not an agreement to stop spying, but to stop spying to assist one's companies. China and the US tacitly agreed that they could continue to spy on each other if there was a national security justification.

China, for both domestic and international reasons, appeared, until recently, to be living up to the 2015 agreement. President Xi wants the PLA to be less corrupt and to focus on military modernization. The agreement reinforces efforts to end PLA units' cybercrime moonlighting to augment their incomes. It advances Xi's goal of centralizing intelligence collection and assets under his control. While the outcome of the 2015 agreement is likely to be a more effective and focused Chinese cyberintelligence effort, so far it appears that Chinese commercial espionage against US companies has decreased.

Results of the Obama-Xi Cyber Espionage Agreement: Intelligence/DoD Perspective

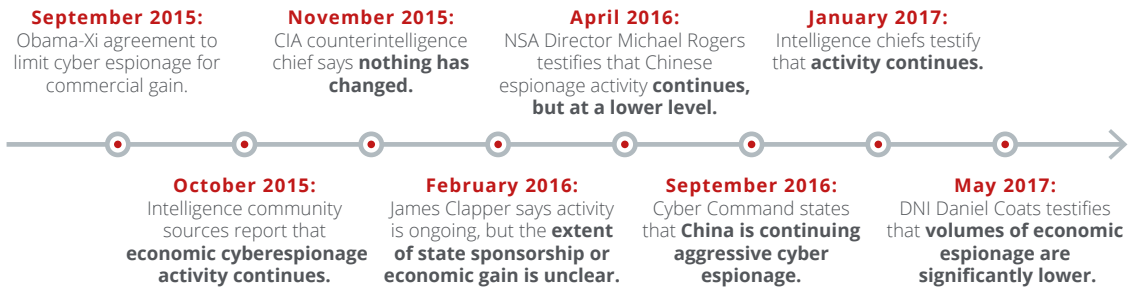


Figure 1. The Obama-Xi Cyber Espionage Agreement.

This "no-commercial-espionage" agreement was endorsed by the G-20, a group of the world's leading economies.[75] The effect on the global cost of cybercrime has been mixed, however. A German official, noting that while Germany and China discussed a ban on commercial espionage, there was never formal agreement and Chinese economic cyberespionage against German companies continues unabated. Based on interviews with officials from a number of countries, IP theft continues unabated despite any agreement.

Putting a value on IP is an art. How much is spent on research and development does not determine the value of IP. Companies can estimate what the IP would fetch on the market if offered for sale or licensing. Companies can estimate the future revenue stream their IP will produce. Extracting information from a computer network does not always mean there is immediate benefit to those who acquire the IP. Many high-tech products require significant "know-how" and experience to produce, and stolen IP alone does not provide that. A thief may not be able to make commercial use of the IP, and there may be a long lag between theft and the introduction of a competing product.

Losses from IP theft are not easy to measure, and it can be difficult to monetize stolen IP. We had a long discussion of the problems of estimating the cost of IP theft in in the 2014 Report. For this 2018 report, we looked at an estimate of the value of the stock of IP and the value of IP created annually. Our estimate puts the value of all IP in the US at $12 trillion, with an annual increase of between $700 billion and $800 billion annually (see endnote). Based on our earlier analyses, and assuming that loss rates from IP theft track other kind of cybercrime and the effect of the Obama-Xi agreement, the annual losses for the US is estimated at between $10 billion and $12 billion from cybercrime targeting IP and perhaps $50 billion to $60 billion globally.

Theft of confidential business information to gain advantage in business negotiations or in investment are an important part of losses from cybercrime, but these may not reflect the full global loss. The hidden cost may come from using hacking to manipulate stock prices, but this kind of cybercrime remains difficult to detect. This kind of manipulation resembles insider trading. An Australian research center estimates the loss from all kinds of market manipulation (including) at about $10 billion a year.[76]

Identity Theft

Surveys routinely show identity theft as one of the top concerns of internet users, not surprisingly, given the size of breaches that routinely make the news. But Bureau of Justice Statistics (BJS) reports in 2012 and 2014 suggest that the actual losses from identity theft remain small. The BJS report found 16.6 million people had experienced some form of identity theft in 2012, resulting losses of about $25 billion. That averages out to $1500 per incident, a painful but not crippling amount for most people. Only 14% of victims suffered out-of-pocket losses, and of those victims, about half lost $99 or less.

A data breach at a leading South African company resulted in the loss of PII for an estimated 31 million people, including the president, finance minister, and police minister. The data included income, address, and phone numbers. The breach left more than half the country's population vulnerable to identity theft.

So why is identity theft such a concern? DOJ found that it was the most expensive kind of property crime the in US, costing $10 billion more than the losses attributed to all other property crime. Second, two-thirds of victims had no idea how or when they had been hacked. Identity theft creates a sense of helpless. An invisible crime that affects millions is something to worry about. Not all identity theft is cyber-related, but the real victims, however, are the banks and credit card companies that bear the bulk of the losses.

Since CSIS's last report, almost three billion internet credentials and other PII have been stolen by hackers. This likely includes duplicates, but the rate of growth over the last five years is staggering. The price of the stolen PII varies with supply and demand, from $50 for health records in 2012 to a few cents for "untested" credit card numbers.[1] There is currently a glut of stolen PII, and, with so much information on the black market, prices are falling.

The breach of credit reporting agency Equifax, which exposed the personal data of 143 million US consumers in September 2017.[2] The most dramatic data breach remains Yahoo, with the loss of a billion individual records. The Equifax breach cost the company nearly $90 million in the first four months after discovery. Equifax incurred a one-time charge related to the cybersecurity incident of $87.5 million, and its net income fell 27% in the third quarter.

Business Email Compromise

Identity theft helps cybercriminals send emails impersonating the CEO or CFO of the company ordering them to make large transfers. In one example, a lower level employee who worked for the CFO received an email from the CEO over the weekend saying that he could not reach the CFO and needed the employee to transfer $10 million immediately to a supplier's new bank account. The employee complied, and the "supplier" account was fraudulent, with the money quickly transferred from it to avoid tracking. The practice has become so prevalent that the FBI instituted a public awareness campaign to warn executives. More than $5 billion has been stolen through these attacks since 2015. The FBI reports that 22,000 businesses worldwide have been victims of business email compromise

Email compromise is difficult for banks to detect and prevent, since the transaction is being submitted by a legitimate, authorized employee of the customer. Some banks are trying to educate customers about the risk, but losses continue to grow. There is also a reluctance to report successful incidents, as companies prefer to absorb the losses.

By 2017, one Russian cybercriminal group amassed the 1.2 billion username and password combinations and more than 500 million email addresses.

Hidden Costs of Cybercrime: Friction and Productivity

Fraud and intellectual property (IP) theft produce much of the loss from cybercrime, but recovery costs (cleaning up after the crime) and opportunity costs, the loss from opportunities or income foregone by the need to spend more on cybersecurity, such as the need for using additional funds for defense that could be spent more productively elsewhere if cybercrime were not so prevalent, are also major contributors. Business interruption is a related cost, often the result DoS attacks and, increasingly, ransomware. In these cases, the loss results from a company being prevented from making money rather than losing money.

In 2014, we predicted increasing opportunity cost for national economies, as people adopt less efficient online behaviors to avoid exposure to cybercrime. According to a 2014 Census Bureau survey of 41,000 American households, 45% percent reported that concerns over cybercrime stopped them from conducting financial transactions, buying goods or services, or posting on social networks.[77] Even though the actual cost and risk may be low, the perception of risk is reshaping how people use the internet in ways that damage economic growth.

That said, people around the world are so entranced with digital technologies that they readily accept risk. It may be that, despite the barrage of news stories, people and companies estimate the risk and cost of being a victim of cybercrime as low and acceptable. A survey we conducted for an earlier report found that many executives viewed cybercrime as "the cost of doing business" and were more concerned with reputational damage than the actual losses.[78] This is changing as corporate and accounting practices takes cyber-risk into account. The expansion of IoT may see opportunity costs increase if people are reluctant to trust future, internet-enabled devices such those used in healthcare devices, smart homes, or self-driving vehicles.

One way to get a sense of the effect of cybercrime is to compare it to the internet economy, the fastest growing segment of the global economy, rather than total global GDP. Recent estimates put the internet economy at $4.2 trillion in 2016.[79] Using this figure, we can see cybercrime as a 14% tax on growth. There would be real benefit to development and prosperity in all countries if the international community made a concerted effort to reduce this.

Selected Country Profiles

We looked at a few countries in each region to illustrate regional and national variation on how cybercrime works. The most disturbing thing we found is that whether a country takes significant efforts against cybercrime or whether it does almost nothing, cybercriminals will still be successful.

Australia

At the end of 2014, the Australian government established an online reporting system for cybercrime in an attempt to improve law enforcement efforts to confront online offenses. Since its inception, the

service recorded more than 114,000 instances of cybercrime, with almost 24,000 coming in the first half of 2017 alone.[80] Australian telecom operator Telstra found that in 2016, almost 60% of businesses were detecting security incidents on at least a monthly basis. This includes the almost one-quarter of businesses that had suffered from a ransomware incident.[81] One particularly damaging segment of cybercrime for Australia is business email compromise, with the Australian government estimating associated losses of more than $15 million over the course of 2016 to 2017.[82] One local council was defrauded out of $340,000 when a cybercriminal sent a series of fake invoices to city councilors over the course of a month.[83] The Australian government has been active in trying to confront this threat, announcing that it would allocate more $170 million in 2016 toward supporting its new National Cyber Security Strategy[84] and proposing legislation that expands the country's anti-money laundering rules to domestic cryptocurrency exchanges.[85]

Brazil

Brazil has one of the most unique cybercrime ecosystems in the world. There is a well-developed community of Brazilian "black-hat" hackers, so much so that courses in spamming and malware implementation are sold openly online.[86] Fifty-four percent of cyberattacks reported in Brazil originate from within the country.[87] Cybercrime is the most common financial crime in Brazil.[88] Banks and financial institutions are common victims, with cybercrime accounting for 95% of losses incurred by Brazilian banks.[89] Consumers are often targeted through look-alike websites, card cloning, and domestically produced malware.[90] In Brazil, more than half of all banking transactions are made with internet-connected devices,[91] but the lack of strong laws against cybercrime is one reason Brazil is both the number-one target and the leading source of online attacks in Latin America.[92] Worldwide, it is the second leading source of attacks and third most-affected target.[93]

Canada

Complaints of cybercrime handled by the Royal Canadian Mounted Police increased 45% between 2014 and last year, evidencing a dramatic increase in cybercrime faced by the Canadian population.[94] According to the Canadian Chamber of Commerce, nearly half of small and medium-size businesses in the country have been the victim of a cyberattack, with cumulative costs to Canada's economy representing billions of dollars a year.[95] At a recent conference, the Canadian director general for federal policing for criminal operations admitted that law enforcement was struggling to adapt to the explosion of cybercrime, saying "The reality is we don't have the resources. We're so busy responding that to get out ahead of the thing is very, very difficult."[96] The Bank of Canada recently warned that the Canadian financial system was highly vulnerable to the cascading effects of cyberattacks, urging new cybersecurity initiatives to prevent the kinds

In October 2016, hackers rerouted the internet traffic of customers attempting to access a major Brazilian bank by gaining control of the bank's DNS. Customers were brought to lookalike sites that collected their personal information and installed malware that disabled customers' antivirus software.

of breaches that could undermine public confidence in the financial system.[97] One recent breach of note was the attack on Canadian payment service provider TIO Networks, owned by PayPal, which exposed the personal and financial information of 1.6 million customers in November of 2017.[98]

Germany

According to German IT industry association Bitkom, more than half of all German companies have been the victims of cybercrime, causing damages of more than $64 billion per year.[99] These costs are rapidly increasing, with the total number of cybercrime instances reported to German law enforcement almost doubling between 2015 and 2016 to a total of 82,000.[100] The head of German federal cybercrime unit has warned that rampant under-reporting of cybercrime means that the true damages are likely far higher than many believe, and others within the German federal police force have called for new legal authorities to enable law enforcement officials to properly confront the problem.[101] Research into the German underground internet economy has shown that the German criminal underground is likely the most developed in the EU, offering a range of goods and services, including a large number of regionally specific offerings. Germany is also a major source of botnets, as shown by the recent arrest of a British hacker for his role in knocking offline almost one million Deutsche Telekom customers after attempting to infect their computers with the Mirai worm.[102]

Japan

The Japanese government does not track cybercrime costs in Japan, but media reports show that the frequency of attacks continues to rise. The most recent statistics available through the National Police Agency show that reports of cybercrime rose to a record level in the first half of 2017, with the almost 70,000 reports representing an almost 5% increase from the previous year.[103] Though Japan had previously been protected from the brunt of the global cybercrime wave due to linguistic barriers and a lack of local infrastructure for money laundering, the country has recently seen a rise in attacks, including several organized attacks targeting major banks.[104]

One of the highest profile attacks in Japan came when criminals breached the Japanese Pension Service and stole 1.25 million records, including ID numbers, names, and birth dates.[105] Ransomware attacks in particular have caused problems for Japanese businesses, with one Kobe University professor speculating that cybercriminals have learned to take advantage of Japanese' willingness to pay the ransoms.[106] While strict criminal laws have discouraged Japanese cybercriminals from widely engaging in malware development, a 2015 investigation of the Japanese cybercrime underground found a robust black market for illegal and counterfeit materials, as well as taboo wares like child pornography.[107]

In May 2015, criminals used stolen information from 3,000 accounts at a South African bank to make 14,000 fraudulent withdrawals from 1,700 ATMs across Japan. The scheme took advantage of 24-hour ATMs that allow withdrawals from foreign credit cards without requiring a chip. In the span of three hours early on a Sunday morning, roughly 100 "withdrawal mules" were able to collect about $17 million in cash.

Mexico

After Brazil, Mexico suffers from the largest number of cyberattacks in Latin America.[108] In 2016, cybercrime cost Mexico an estimated $3 billion dollars in economic damages,[109] with the Mexican Federal Police reporting that they had dealt with more than 120,000 cybersecurity cases during the current administration.[110] Law enforcement actions to mitigate cybercrime are complicated in Mexico due to a lack of legal tools and poor enforcement of existing laws These two factors have led to Mexico becoming a haven for stolen personal data.[111] Poor investment in cybersecurity has also hurt the country, which recently found itself the target of state-sponsored cybercrime when the North Korean hacking group Lazarus attempted to steal money from Mexican banks in 2016.[112]

United Kingdom

Online fraud and cybercrime are the most common crimes in the UK, with the more than 5.5 million yearly offenses estimated to account for nearly half of all crime in the country.[113] Government figures indicate that almost half of all UK businesses suffered a cyberattack or data breach in 2016, with the costs ranging from an average of $26,700 up to a maximum of millions of dollars in the most damaging instances.[114] The UK government has been active in confronting the threat, announcing in November 2016 a National Cyber Security Strategy that would invest over $2.5 billion in strengthening law enforcement capabilities and in educating a new generation of cybersecurity experts.[115] The cyberhazard to the UK was dramatically demonstrated this past May, when more than one-third of National Health Service trusts were victimized by the WannaCry ransomware campaign, causing almost 7,000 appointments and operations to be canceled as doctors scrambled to serve patients in the face of a technical blackout.[116]

United Arab Emirates

According to the UAE Cyber Security Centre, the UAE is the second most targeted country in the world for cyberattacks.[117] The country's high internet penetration, technological sophistication, and highly visible profile have been cited as reasons for the high cost of cybercrime for the UAE, estimated at $1.4 billion per year.[118] According to a survey conducted by UAE telecom du, at least 40% of residents have been the victim of a cybercrime,[119] with research showing that more than three quarters of those who lose money through online crime are never able to get that money back.[120] After Saudi Arabia, the UAE is the most targeted Gulf country for both ransomware and botnet sources.[121, 122] The country recently established a new federal public prosecution to handle cybercrimes, reflecting the government's increasing interest in reigning in the costs to its citizens.[123]

What Can Be Done?

This report focused on estimating the cost of cybercrime, not on recommendations on how to deal with cybercrime, but several steps are obvious from our cost analysis.

- Uniform implementation of basic security measures (like regular updating and patching and open security architectures) and investment in defensive technologies—from device to cloud—remain crucial. Protection against most cybercrimes does not require the most sophisticated defenses. This responsibility mainly falls on companies and consumers.
- The need for increased international law enforcement cooperation is obvious, both with other nations' law enforcement agencies and with the private sector, but with this comes a requirement for additional resources for investigation and to expand agency resources, and for cybercrime capacity building in developing nations.
- This includes improving existing processes, such as the Mutual Legal Assistance Treaty (MLAT). MLATs allow one government to request the help of another in investigating cybercrime or in obtaining evidence. MLATS were created for the pre-internet era, are inadequate, and need to be modernized or replaced._
- As we have said repeatedly in this report and in earlier reports, improved collection of aggregate by national authorities is essential.
- Greater standardization (threat data) and coordination of cybersecurity requirements would improve security, particularly in key sectors like finance.
- Nation-states with inadequate cybercrime laws face higher rates of cybercrime and create problems for their neighbors. The Budapest Convention, a formal treaty on cybercrime, defines state responsibilities for enforcement and cooperation, but the Budapest Convention has made slow progress in the face of opposition from Russia and other countries. Russia claims the treaty is intrusive and may also have little interest in curtailing Russian criminal groups. China, Brazil, and India also refuse to sign the treaty on the grounds that they were not involved in its negotiations. Waiting to negotiate a new convention will slow any progress in reducing cybercrime.
- Finally, the state sanctuaries for cybercrime must come under pressure from the international community to change their behavior and cooperate with other nation's law enforcement agencies. This means imposing some kind of penalty or consequence on governments that fail to take action against cybercrime. In the case of Russia and North Korea, we have exhausted the portfolio of sanctions, and new penalties must be devised— penalties that are painful, but temporary and reversible.

Without these kinds of action, cybercrime will continue to grow as the number of connected devices grows and as the value of online activities increases. Better data collection on cybercrime is essential for scoping the problem and justifying additional resources. Data collection can be a thorny political issue for some countries, as victims would often prefer not report cybercrime. It can also be difficult to quantify the value of intangible goods and services and some financial cybercrimes, such as stock market manipulation, may be currently undetectable. Despite all the attention given to cybersecurity, its transnational nature and the complexity of the technology (which affects evidence collection) make it a difficult problem for any country to manage.

This makes cybercrime part of a larger problem, as nations undergo the digital revolution that has changed business, politics, security, and law enforcement. Our ability to govern this digital revolution has lagged. Accounting is one of the most basic functions of government, allowing nations to systematically acquire information that helps them govern and provide services to citizens. Better accounting for cybercrime will be essential for the digital world into which we are moving. Estimating the cost of cybercrime can start to help the world manage and reduce cybercrime, a task whose importance will only grow as our reliance on digital technologies grows and as cybercrime grows with it.

Valuing intellectual property: The most recent estimate of IP stock value comes from 2011, where it was estimated to be between $8.1 and $9.2 trillion (up from $5 trillion to 5.5 trillion in 2005). To estimate the value of IP stock, the authors calculated the total value of intangible assets held by publicly traded US firms (both on-balance and off-balance sheet value) and then multiplied it by a Federal Reserve estimate of the share of intangible assets representing intellectual capital.

Using an adjustment of the authors' method (explained below), we estimate the current value to be $12.8 trillion. According to data from the Bureau of Economic Analysis, private investment in intellectual property products (software, R&D, and creative/entertainment products) will be more than $800 billion in 2017. Software and R&D accounts for 89.2% of IP products. To estimate the total value of intangible assets, we multiplied the total value of all publicly traded US firms ($27.352 trillion as of 2016, according to the World Bank) by a 2015 estimate of the share of S&P 500 market value represented by intangible assets (84%, according to IP merchant bank Ocean Tomo). Then we multiplied this number by the authors' 2011 update of the Federal Reserve estimate of the share of intellectual assets that represent intellectual capital (55.8%). This last number is undoubtedly the weakest link in the calculation, but we cannot find an updated figure.

1. Jane Chong, "Why is Our Cybersecurity So Insecure?," New Republic, October 11, 2013
2. www.imf.org/external/pubs/ft/sdn/2016/sdn1605.pdf
3. "Americans and Cybersecurity" Pew Research Center, January 26, 2017
4. https://www.reuters.com/article/us-russia-cyber-arrests-factbox/factbox-u-s-arrests-of-russian-cyber-criminals-hit-record-high-idUSKCN1B50M5
5. Virginia Harrison and Jose Pagliery, "Nearly 1 million new malware threats released every day," CNN, April 14, 2015
6. http://docs.apwg.org/reports/apwg_trends_report_q3_2016.pdf
7. https://cointelegraph.com/news/north-korea-accused-of-hacking-south-korean-bitcoin-exchange-youbit
8. https://www.rferl.org/a/greek-court-extradition-vinnik-russia-cybercrime/28914225.html
9. https://www.mcafee.com/de/resources/reports/rp-economic-impact-cybercrime2.pdf
10. https://data.worldbank.org/indicator/NY.GDP.MKTP.CD; http://databank.worldbank.org/data/download/GDP.pdf
11. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx
12. http://www.telegraph.co.uk/news/2016/11/01/how-much-of-a-problem-is-cyber-crime-in-the-uk/
13. http://oceansbeyondpiracy.org/publications/economic-cost-somali-piracy-2012, http://oceansbeyondpiracy.org/sites/default/files/attachments/The%20Economic%20Cost%20of%20Piracy%20Full%20Report.pdf
14. http://www.unodc.org/unodc/en/frontpage/2012/October/transnational-crime-proceeds-in-billions-victims-in-millions-says-unodc-chief.html
15. http://www3.weforum.org/docs/WEF_State_of_the_Illicit_Economy_2015_2.pdf
16. http://www.gfintegrity.org/wp-content/uploads/2017/03/Transnational_Crime-final.pdf
17. "Things to do before the next big thing: How the financial industry reacts to cyberthreats," Kaspersky, March 9, 2017
18. "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," US Department of Justice Office of Public Affairs, March 24, 2016
19. Elias Groll. "NSA Official Suggests North Korea Was Culprit in Bangladesh Bank Heist." Foreign Policy, March 21, 2017. http://foreignpolicy.com/2017/03/21/nsa-official-suggests-north-korea-was-culprit-in-bangladesh-bank-heist/
20. Danny Palmer. "New wave of cyberattacks against global banks linked to Lazarus cybercrime group." ZDNet, February 13, 2017. http://www.zdnet.com/article/string-of-cyberattacks-against-global-banks-linked-to-lazarus-cybercrime-group/
21. Dmitry Volkov. "Lazarus Arisen: Architecture, Techniques and Attribution." Group-IB, March 30, 2017. http://www.group-ib.com/lazarus.html
22. Luke McNamara, "Why Is North Korea So Interested in Bitcoin?," FireEye, September 11, 2017
23. Joon Ian Wong, "North Korea could be secretly mining cryptocurrency on your computer," Quartz, October 24, 2017
24. David Gilbert, "North Korea's bitcoin crash course has experts worried," Vice, November 25, 2017
25. Symantec Security Response. "SWIFT attackers' malware linked to more financial attacks." Symantec Connect, May 26, 2016. https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks
26. Danny Palmer. "New wave of cyberattacks against global banks linked to Lazarus cybercrime group." ZDNet, February 13, 2017. http://www.zdnet.com/article/string-of-cyberattacks-against-global-banks-linked-to-lazarus-cybercrime-group/
27. http://www.independent.co.uk/news/uk/crime/russia-hacking-threat-uk-number-one-warning-cyber-attacks-wannacry-north-korea-iran-investigations-a8061521.html
28. https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions
29. Max Metzger. "FBI says Ransomware soon becoming a billion dollar business." SC Media UK, January 10, 2017. https://www.scmagazineuk.com/fbi-says-ransomware-soon-becoming-a-billion-dollar-business/article/630615/
30. "McAfee Labs Threat Report," McAfee, December 2017,
31. Alina Simone, "The Strange History of Ransomware," Public Radio International, May 17, 2017
32. Imperva. "The Secret Behind CryptoWall's Success." Imperva Hacker Intelligence Initiative, 2016. https://www.imperva.com/docs/IMPERVA_HII_CryptoWall_report.pdf
33. Federal Bureau of Investigation. "GameOver Zeus Botnet Disrupted: Collaborative Effort Among International Partners." June 2, 2014. https://www.fbi.gov/news/stories/gameover-zeus-botnet-disrupted
34. CERT-UK. "Is ransomware still a threat?" May 16, 2017. https://c.ymcdn.com/sites/misaontario.site-ym.com/resource/resmgr/Ontario_Documents/Is_ransomware_still_a_threat.pdf
35. Carbon Black, "The Ransomware Economy," October 2017
36. Barkly, "Ransomware-as-a-Service is Booming: Here's What You Need to Know," March 2017
37. Dorka Palotay, "Ransomware as a Service (RaaS): Deconstructing Philadelphia," Sophos, July 25, 2017
38. Armada Cloud, "The State of Ransomware in 2016: Ransomware Statistics Infographic," 2016
39. Elad Erez, "What's Next for Ransomware: Data Corruption, Exfiltration and Disruption," Imperva, May 16, 2017
40. Carbon Black, "The Ransomware Economy," October 2017
41. Trend Micro, "Forecasting the Future of Ransomware," July 24, 2017
42. https://www.washingtonpost.com/news/business/wp/2017/09/20/sec-reveals-it-was-hacked-information-may-have-been-used-for-illegal-stock-trades/?utm_term=.6898421180d9
43. Malwarebytes, "The New Mafia: Gangs and Vigilantes," December 7, 2017
44. Europol, "Internet Organised Crime Threat Assessment 2017," 2017
45. Carbon Black, "The Ransomware Economy," October 2017

46. Limor Kessem, "Dark Web Suppliers and Organized Crime Gigs," IBM Security Intelligence, February 11, 2016
47. Carbon Black, "The Ransomware Economy," October 2017
48. Europol, "Internet Organised Crime Threat Assessment 2017," 2017
49. Office of Public Affairs, "AlphaBay, the Largest Online 'Dark Market,' Shut Down," Department of Justice, July 20, 2017

50. Mathew Schwartz, "How Do We Catch Cybercrime Kingpins," Data Breach Today, June 4, 2015
51. Carbon Black, "The Ransomware Economy," October 2017
52. Raj Samani and Francois Paget, "Cybercrime Exposed: Cybercrime-as-a-Service," McAfee, 2013
53. Charlie Osborne, "Shadow Brokers launch subscription service for stolen exploits, zero-day leaks," ZDNet, May 31, 2017
54. Symantec, "Internet Security Threat Report Volume 22," April 2017
55. Lucian Constantin, "Cost of a Windows zero-day exploit? This one goes for $90,000," CSO Online, June 1, 2016
56. Graham Cluley, "Yahoo's billion account database for sale on the black market," Bitdefender, December 2016
57. Limor Kessem, "Dark Web Suppliers and Organized Crime Gigs," IBM Security Intelligence, February 11, 2016
58. Europol, "Internet Organised Crime Threat Assessment 2017," 2017
59. Pierluigi Paganini, "A day attack with DDoS booter cost $60 and can cause $720k in damage," Security Affairs, March 4, 2016
60. Denis Makrushin, "The cost of launching a DDoS attack," Kaspersky, March 23, 2017
61. Symantec, "Internet Security Threat Report Volume 22," April 2017
62. Nicky Woolf, "DDoS attack that disrupted internet was largest of its kind in history, experts say," The Guardian, October 26, 2016
63. Europol, "Internet Organised Crime Threat Assessment 2017," 2017
64. Aaron van Wirdum, "Is Bitcoin Anonymous? A Complete Beginner's Guide," Bitcoin Magazine, November 18, 2015
65. Russell Brandom, "Bitcoin exchange chief arrested amid new questions about Mt Gox theft," The Verge, July 26, 2017
66. John Bohannon, "Why criminals can't hide behind Bitcoin," Science, March 9, 2016
67. Emerging Technology from the arXiv, "Bitcoin Transactions Aren't as Anonymous as Everyone Hoped," MIT Technology Review, August 23, 2017
68. Andy Greenberg, "Monero, the Drug Dealer's Cryptocurrency of Choice, is on Fire," Wired, January 25, 2017
69. Charles Bovaird, "What Investors Should Know Before Trading Zcash," CoinDesk, November 27, 2016
70. Kyle Torpey, "AlphaBay Comments on Bitcoin Congestion, Monero Adoption and Zcash Possibilities," Bitcoin Magazine, December 21, 2016
71. Europol, "Internet Organised Crime Threat Assessment 2017," 2017
72. Andy Greenberg, "The Fed-Proof Online Market OpenBazaar is Going Anonymous," Wired, March 6, 2017
73. Europol, "Internet Organised Crime Threat Assessment 2017," 2017
74. David E. Sanger, "Chinese Curb Cyberattacks on U.S. Interests, Report Finds," New York Times, June 20, 2016
75. G20 Leaders' Communiqué, Antalya Summit, 15-16 November 2015 http://www.mofa.go.jp/files/000111117.pdf
76. https://www.thetradenews.com/Trading---Execution/Regulation/Market-manipulation-cost-global-markets-US$3-4-billion-in-Q2/
77. https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities
78. https://www.mcafee.com/us/security-awareness/articles/misaligned-incentives.aspx
79. https://www.bcg.com/documents/file100409.pdf
80. Office of the Prime Minister, "Offensive Cyber Capability To Fight Cyber Criminals," June 3, 2017
81. Neil Campbell and Berin Lautenbach, "Telstra Cyber Security Report 217," March 30, 2017
82. Australian Cyber Security Centre, "2017 Threat Report," October 2017
83. Trend Micro, "Brisbane Council Loses 450K AUD to BEC Scam," August 25, 2016
84. Office of the Prime Minister, "Offensive Cyber Capability To Fight Cyber Criminals," June 3, 2017
85. Stan Higgins, "Australia Takes Aim at Cryptocurrencies With New Money Laundering Bill," Coindesk, August 17, 2017
86. Fabio Assolini, "A School for Cybercrime: How to Become a Black Hat", Secure List, January 16, 2012
87. Incidentes Reportados ao CERT.br – Janeiro a Dezembro de 2015
88. Kessem
89. Nicole Perlroth, "Cybercrime Scheme Uncovered in Brazil", The New York Times, July 2, 2014
90. Kerry Tomlinson, "How Crooks are Pulling Off Brazil Olympics Scams", Archer News, June 14, 2016
91. Deloitte, "Pesquisa FEBRABAN de Tecnologia Bancaria 2015", FEBRABAN, 2015
92. Limor Kessem, "Meet the Pezao Trojan: Brazil's Got Malware", Security Intelligence, May 13, 2015
93. Gustavo Diniz, "Deconstructing Cyber Security in Brazil: Threats and Responses", Igarape Institute, December 2014
94. Howard Solomon, "Canadian police frustration over cyber crime shows at conference," IT World Canada, November 7, 2017
95. Guillaum Dubreuil, "Canadian Businesses Lose Billions of Dollars to Cyber Crime Each Year," Canadian Chamber of Commerce, March 4, 2017
96. Howard Solomon, "Canadian police frustration over cyber crime shows at conference," IT World Canada, November 7, 2017
97. Mike Blanchfield and Jim Bronskill, "Bank of Canada warns financial sector vulnerable to cyberattacks," CBC News, June 13, 2017
98. Pierluigi Paganini, "PayPal-owned company TIO Networks data breach affects 1.6 million customers," Security Affairs, December 3, 2017
99. "In the last two years over half of German companies have been hit by sabotage," Business Insider, July 21, 2017
100. Andrea Shalal, "Germany sees rise in cybercrime, but reporting rates still low," Reuters, May 3, 2017
101. "Germany needs tougher laws against cyber crime, top policeman tells paper," Reuters, August 5, 2017

102. Alistair Walsh, "Deutsche Telekom hacker very sorry for botnet attack on a million internet users," DW, July 28, 2017
103. "Cybercrime reports climb to a record in first half of 2017," Japan Times, September 7, 2017
104. Limor Kessem, "Organized Cybercrime Big in Japan: URLZone Now on the Scene," IBM Security Intelligence, February 1, 2016
105. Tomoko Otake, "1.25 million affected by Japan Pension Service hack," Japan Times, June 1, 2015

106. Ichiro Kitamoto, "Computer ransomware that locks out users flourishes in pay-to-make-it-go-away Japan," Japan Times, March 12, 2017
107. Akira Urano, "The Japanese Underground," Trend Micro, October 13, 2015
108. Luisa Parraguez Kobek, "The State of Cybersecurity in Mexico: An Overview," The Wilson Center, January 2017
109. Itzel Castanares, "Cybercrime costs Mexico 3 billion dollars a year," El Financiero, July 9, 2016
110. Luisa Parraguez Kobek, "The State of Cybersecurity in Mexico: An Overview," The Wilson Center, January 2017
111. Tristan Clavel, "Mexico Struggling with Widespread Cyber Theft of Personal Data," InSight Crime, December 7, 2016
112. Pierluigi Paganini, "Watering hole attacks on Polish Banks Linked to Lazarus Group," Security Affairs, February 13, 2017

113. Martin Evans and Patrick Scott, "Fraud and cyber crime are now the country's most common offences," The Telegraph, January 19, 2017
114. UK National Cyber Security Centre, "Almost half of UK firms hit by cyber breach or attack in the past year," April 19, 2017
115. UK Cabinet Office, "Britain's cyber security bolstered by world-class strategy," November 1, 2016
116. "NHS 'could have prevented' WannaCry ransomware attack," BBC News, October 27, 2017
117. Mark Nituma, "8 Most Common Cybercrimes in the UAE," 999 Security and Safety for All, March 2017
118. Naushad Cherrayil, "Cybercrime cost UAE Dh5.14b this year," Gulf News, November 22, 2016
119. Caline Malek, "Two in five are cyber crime victims," The National, November 12, 2016
120. "Online financial cybercrime victims in the UAE struggle to recover all their lost money," Albawaba Business, February 1, 2017
121. "High incidence of ransomware cyber attacks in UAE," Khaleej Times, May 4, 2017
122. Mahsoom Thottathill, "Riyadh, Dubai, lead GCC's Top Botnet Cities," Arabian Gazette, October 31, 2017
123. Omar Khodeir, "UAE Introduces New Public Prosecution Focusing on Cyber Crime," Tamimi, March 12, 2017

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

About CSIS

Established in Washington, D.C., over 50 years ago, the Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to providing strategic insights and policy solutions to help decision makers chart a course toward a better world.

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. CSIS is regularly called upon by Congress, the executive branch, and the media to explain the day's events and offer bipartisan recommendations to improve U.S. strategy.

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com