The impact of cyberterrorism on the us economy essay example

Business, Company

IMPACT OF CYBER-TERRORISM TO THE US ECONOMY

Impact of Cyber-Terrorism to the US Economy

It is disturbing to think nowadays how computers are now used by politically motivated international and national insurgent or terrorist groups as weapons against the people for the sake of their ideology. With just one click, these groups can easily shut down critical infrastructure in any part of the globe, paralyzing the entire country in seconds. Consequently, the impacts of these attacks are very severe to the country that leaves the government and the people intimidated or scared of these groups. Since the first wave of cyber-attacks were done by terrorists and insurgent groups, research has been done extensively to try countering this threat. As it is a new field of study, literature is quite limited with regards to the overall nature and impact of cyber-terrorism. Regardless of this lack of literature, cyber-terrorism has the capacity to cripple the US economy by the loss of crucial information, financial loss, stock market manipulation, opportunity costs, high security expenses and reputational damage that can discredit the US market.

Since the introduction of the internet and its many features, many economies throughout the globe have greatly benefitted through its use. According to Censky (2012) the internet contributes to almost all major economies in the globe, especially in the United States. The study done by the Boston Consulting Group indicated that the internet has given a total revenue of $684 billion or 4. 7% to the US’ overall economic activity in 2010 in comparison to the $625 billion contribution of the federal government. If

the internet was a separate sector, the study indicated that it would be larger in comparison to the US' education, construction and agricultural sector considering its influence to the economy. In retail, for example, e-commerce is now a popular medium for US businesses, contributing to 5% of total US sales since 2010. Most Americans have even stressed that they are willing to give up almost anything for the internet and the study had showed that Americans see the internet to be worth $3, 000 each year . Given this high importance, any attack to the internet infrastructure of the country by any group or individual may be very dangerous and for the economy, this spells disaster and severe impacts.

One of the major points considered by experts with regards to a possible threat to the internet infrastructure of the country are cyber-terrorists. Cyber-terrorism has long been a problem for the United States since the introduction of the internet in the 1990s. Weimann (2004) cited that the National Academy of Sciences reported that since Americans rely heavily on computers, there is a high likelihood that terrorists would exploit this fact to disable the country without using bombs. In the report of the NAS released to support this claim, the NAS cited that cyber-terrorism can be considered " the electronic Pearl Harbor" that would only raise more fear and terror to the American people as it can devastate the country similarly to the surprise attack of the Japanese, especially on the sectors in which the attack had concentrated into to cause trauma. By the time 9/11 had happened, experts and policy-makers alike had thought the al Qaeda would now utilize the cyberspace as a new battleground for their initiative against their targets. Debates had followed suit as to how national security can be protected by

the government from possible cyber-attacks due to the conflicting positions of the government. Experts have continued to argue that cyber-terrorism would easily take out any country as it utilizes the internet to spread terror and stop all operations. With America’s major services and operations concentrated on the net, cyber-terrorist, experts analyzed that terrorists would love to exploit this territory and get high media coverage they desire with their cyber-attack .

According to the research of the Center for Strategic and International Studies (2013), the impact of cyber-terrorism to the US economy can range from loss of crucial information, financial loss, stock market manipulation, opportunity costs, high security expenses and reputational damage that can discredit the US market. For the first impact, cyber-terrorists can instigate economic espionage in any company or financial institution for intellectual property patents and business-confidential information. These terrorists would take these stolen information – from product plans to customer information – and leak it to other companies. While the information would still remain in the hands of the company, they will not be able to identify if the information is still secured or is already transmitted to other companies or individuals. Intellectual property can be difficult to put into value as it would depend on the estimated income streams and production estimates. If a company’s product plan is stolen by another company and becomes successful, the loss of the original company would be equal to the investment they had on the product. In the case of a US company with $1 billion in intellectual property, the competitor with the leaked information would now have access to crucial product information without paying and

reproduce the product which is cheaper than the original product .

Cyber-terrorists can also use their stolen information and money to influence and manipulate the stock market. In the testimony of Assistant Director Gordon Snow of the FBI (2011), cyber criminals mostly utilize their resources to target securities and brokerage firms to influence the market and conduct unauthorized stock trading. In 2010, the FBI and other law enforcement agencies of the country have observed that cyber-terrorists have utilized unauthorized financial transactions from a victim bank or brokerage account while being paired with a Telephone Denial of Service attack to spam the victim’s phone number to prevent verification of the transaction. Several reports of unauthorized online withdrawals have been indicated throughout the country, especially on high-profile financial targets. In July 2009, for example, two U. S. stock exchanges were victims of DDoS attacks, removing access to their public website that would stop their services to the public even if the financial market continues to persist. In February 2011, cyber-terrorists have used online advertisements to spread malicious software on the public site of a foreign stock exchange in the country, tricking users in paying for the software. NASDAQ had also reported high security breaches by unauthorized intruders in their main web application reserved for high ranking traders and officials used for their confidential information sharing program. These incidents, according to Snow, indicate that cyber-criminals now have the capacity on affecting real time operations without alarming the authorities .

The economy would also lose severe amounts of opportunities from cyber-terrorism due to immense number of service disruptions and cancellations

caused by malicious viruses and ‘ missing’ websites. Denial of services from e-commerce sites or financial institutions would cause a drop of sales as consumers would defer their requests and go to another provider. In some instances, it would lead to consumers to avoid the internet and lower their value activities that would disrupt many e-commerce websites in the country. Another prominent opportunity cost that would impact the country due to cyber-terrorism is the effect of innovation towards the receiving country. While the receiving company or country of stolen information and goods would improve their ability to produce goods, it would cause disincentives in the recipient country and restrict their technological improvement. The recipient country would also find itself unable to innovate fully, reducing their resources and possibility lose international business partnerships and domestic businesses alike . In addition to this, the National Research Council (2011) cited that cyber failure can cause many areas to lose access to crucial services such as electricity and government services, which may cause a wide-area blackout that can amount to $2 trillion worth of recovery costs. In a 2001 report for the US Department of Transportation, they had also cited that any attack on the global positioning system (GPS) of various institutions and infrastructure that controls transportation may disrupt product deliveries and promptness for some companies relying on transportation that can reach up to $8 billion losses. American news outfits have repeatedly reported various instances wherein cyber-terrorists have used their GPS jammers (which can be bought online) to confuse national channels, especially for those relying on GPS for logistics and communication

.

With the loss of crucial information through cyber-terrorist attacks and the resulting impacts it has on the stock market and the services the US economy provides, the expense it has is quite troubling for both consumer and companies affected. For consumers, Guard and Guard (2001) cited that they would become infected with worms and viruses that would allow terrorists to both gain information from the victim's computer and use the information to exploit the victim. One of the most notable examples of viruses used by political hacktivism and cyber-terrorists was the virus known as " wtc. txt. vbs" which would allow them to control the computer by spreading the virus and target the country's internet infrastructure. These terrorists can move money out of victim's accounts, compromise their confidential data, establish online bill payments to their dummy accounts, and even use the information to threaten the consumer/victim in question. In addition to this, hackers or cyber-terrorists can fake domain name servers (DNS) to trick the customer who would be viewing their online banking accounts into a fake or dummy website to copy their information for their use . According to the CSIS (2013), identity theft in the US has already amounted to $780 million worth of losses. In the case of US banks and other financial institutions, it is estimated that they are also losing almost $300 million to $500 million each year due to cyber-attacks.

In addition to this, companies would also have to pay millions of dollars for network protection and security to protect themselves from cyber-attacks in the future. It is predicted that governments and companies around the globe spend 7% of their budgets for information technology security and cyber-security software. Each year, at least $60 billion is used for cyber security

software throughout the globe. In the case of the United States, the US Office of Management and Budget reported that in 2012, federal agencies had utilized $15 billion worth of budget for their cyber-security efforts or almost 20% of the entire federal budget for information technology. Companies are also spending the same amount for cyber-security measures amounting to almost $ 1 billion each year. Cleaning up after cyber-attacks can also be quite expensive as large companies would often use $9 million to replace their entire infrastructure and materials and insurance . In terms of insurance, Cashell, et al (2004) cited that the insurance industry is greatly affected by these cyber-attacks as these companies would now have to adjust their premiums to cover cyber-risks, which can damage their business. Several insurance companies, such as AIG, Chubb, St. Paul and Ace Ltd, had to revise their traditional business insurance coverage to include cyber-risk policies amounting to almost $120 million in 2002 and this is estimated to increase as high as $6 billion by 2006. While insurance companies are aware of the risks of handling cyber-insurance, they are unable to ensure how much coverage they will offer to their customers and disable immediate response to these risks. While these insurance companies provide accurate results on the possible damages these attacks would incur, successfully pricing insurance premiums is tricky as these attacks may differ in severity in the next couple of years .

Finally, with cyber-terrorism disabling the company’s operations and affecting customer or business partner satisfaction, cyber-terrorism has the capacity to destroy a company or financial institution’s reputation. For companies, losing their reputation is very dangerous as it would lead to

immense losses and drops on their stock prices. Companies who have been devaluated or suffering from immense scrutiny and attacks find their stock prices drop from 1% to 5% unless they revised their services before the next quarter. Regardless of this, this would cause stockholders to have second thoughts on maintaining their investments in the company, especially if the company reported heavy damage in their portfolio and high outflow of customers . As a result, they will lose their credentials and their support.

In addition to this, Guard and Guard (2001) cited that if the American public becomes aware of a company or a financial institution’s weakness, they would slowly question the integrity and confidentiality of their information stored by these institutions or companies. In the statement of National Intelligence Officer for Science and Technology Lawrence Gershwin in June 2001 for the Joint Economic Committee of Congress, he stressed that highly publicized intrusions and virus attacks such as those in the California Independent System Operator – which handles 75% of California’s electricity – had aided in the negative perceptions of the public regarding the US government’s capacity to protect national security and the country’s economic well-being. The fear of the public had drastically been exaggerated to the extent that the public is now distrustful of the benefits of technology . Unless something is done with these impacts, the US economy may find itself vulnerable to various attacks against future cyber-attacks from groups wanting to disrupt the US’ growth and stability.

In today’s developing world, countries with the strongest network infrastructure and open and secure access to the internet have an advantage. For the US, this holds true as the world’s economy and balance

rest in America’s stability and growth. However, with the growing threat of cyber-terrorism, even the US finds itself vulnerable to the possibilities of losing control from the cyber-terrorists wishing to dislodge the balance and spread fear and violence in the country. Not only would these attacks constitute to financial losses for the government, it would also lose the trust and loyalty of the people – and of investors and companies- to the capacity of the US government and its institutions to protect them from these types of attacks. The necessity of finding solutions to counter cyber-terrorism is now vital to not only ensure political and security freedom, but also economic sustainability as the internet is now growing to fit the now digitalized developing world.

References

Cashell, B., Jackson, W., Jickling, M., & Webel, B. (2004). The Economic Impact of Cyber-Attacks. Washington, D. C.: US Library of Congress, Congressional Research Service.

Censky, A. (2012, March 19). Internet accounts for 4. 7% of U. S. economy. Retrieved from CNN Money: http://money. cnn. com/2012/03/19/news/economy/internet_economy/

Center for Strategic and International Studies. (2013). The Economic Impact of Cybercrime and Cyber Espionage. Santa Clara: McAfee.

Guard, M. B., & Guard, M. (2001, October 12). Physical and Digital Threats to Financial Institutions in the Wake of the Terrorist Attacks. Retrieved from BankersOnline: http://www. bankersonline. com/security/cyberthreats. html

National Research Council. (2011). Building Community Disaster Resilience

Through Private-Public Collaboration. Washington, D. C.: National Academies Press.

Snow, Gordon. (2011, September 14). The Cyber Threat to the Financial Sector. Retrieved from Federal Bureau of Investigation: http://www. fbi. gov/news/testimony/cyber-security-threats-to-the-financial-sector

Weimann, G. (2004). Cyberterrorism: How Real is the Threat? Washington, D. C.: United States Institute of Peace.