The Eurasia Center/EBC Brief

The Effects of Cyber-attacks on International Business

February 2021

Cybersecurity and Business Photo Credit: Forbes

Keeret Heer
The Eurasia Center

www.EurasiaCenter.org

The Eurasian Business Coalition (EBC)
www.eurasianbusiness.org www.usebc.org

The Effects of Cyber-attacks on International Business

Image of Cybercriminal: Discovery Labs

Cyber-attacks are not a new concept, the first known cyberattack that took place in 1988 was accidental. The Morris Worm, developed by Robert Morris, intended to assess the size of the internet, installed itself on each targeted computer and debilitated the system, eventually causing the computer to crash. It destroyed over 6000 computers which at that time made up approximately 10% of the internet. The damage was estimated to be between USD 100,00-1 million (FBI, 2018). Today, cyberattacks ravage critical infrastructure systems, causing

damages in the tens of millions. Since 2009, there has been a 66% YoY compounded increase in cybersecurity events (Tweneboah-Kodua, 2).

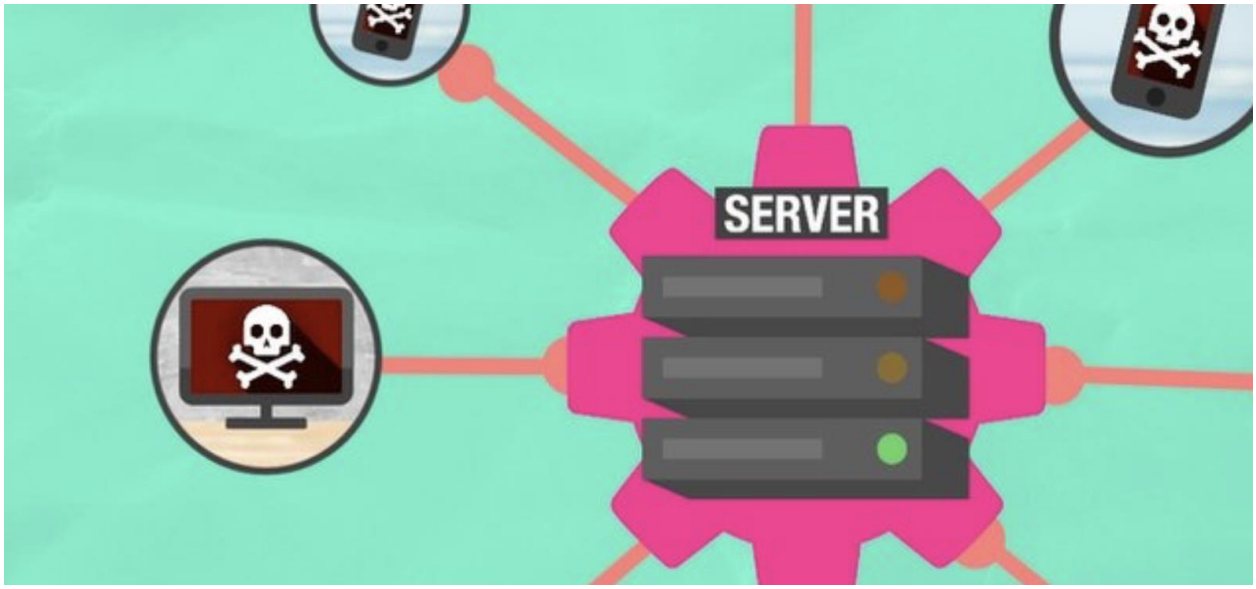
The damage extends from the physical into the financial sphere, thus impacting businesses negatively from virtually all directions. This also harms the stock values of such corporations. In 2014, the global cost of cybersecurity-related events was pegged at USD 24 billion (Tweneboah-Kodua, 4). Such a value is attributed to decreased revenue, production loss, lawsuits, regulatory penalties, loss in customer base, etc. Different sectors have different levels of vulnerability to cyberattacks. Healthcare, retail, public sector undertakings, technology, education, and energy are the most vulnerable sectors. For the healthcare industry, ransomware is the biggest threat, putting millions of patient records at risk of being sold off.

The Times of India, 2017

The energy sector is extremely vulnerable to attacks as close-range devices can penetrate their systems with ease. U.S. natural gas pipelines are regularly targeted with the recent Colonial Pipeline attack of 2021 resulting in a ransom of USD 5 million. The attack led to a cessation of services for 5 business days, leading to strained supply lines throughout the U.S. the supplies of jet fuel, diesel, and petrol tightened, resulting in the average price per gallon to hit $3.008, the highest since 2014 (BBC, 2021). Higher education faces the risk of identity theft as well. Since 2010, universities have experienced the highest number of cyber-attacks, with 539 breaches affecting around 13 million records (CDNetworks, 2021). The financial sector also suffers greatly from cyberattacks. Securities and Brokerage firms are confronted by regular attacks, the results of which are stolen identities, unauthorized trades, and so on. The banking sector has come under fire from a wave of attacks since the beginning of the Covid-19 pandemic. Such attacks put the respective banks at risk of a rating downgrade, thus the institution would only be able to borrow funds at a higher cost. This would usually be accompanied by reduced investor confidence in the business, thus making it harder for the organization to raise funds. This has a direct effect on the profitability of the company (Kotak Securities, 2020).

BBC, 2021

The Covid-19 Pandemic, by thrusting onto the world a work-from-home model, has catalyzed the digital transformation plans of many businesses. This dramatic transition was taken advantage of by many hackers, who spotted the loopholes of the programs and used them to their advantage. The main threats that businesses face is from the following four kinds of cyber-attacks. Firstly, are Supply Chain Attacks, through which the hacker gains access by compromising the organization's supply chain. 2020 saw a massive supply chain attack occur when software provider SolarWinds was hit and thus compromised. This led to attacks on their

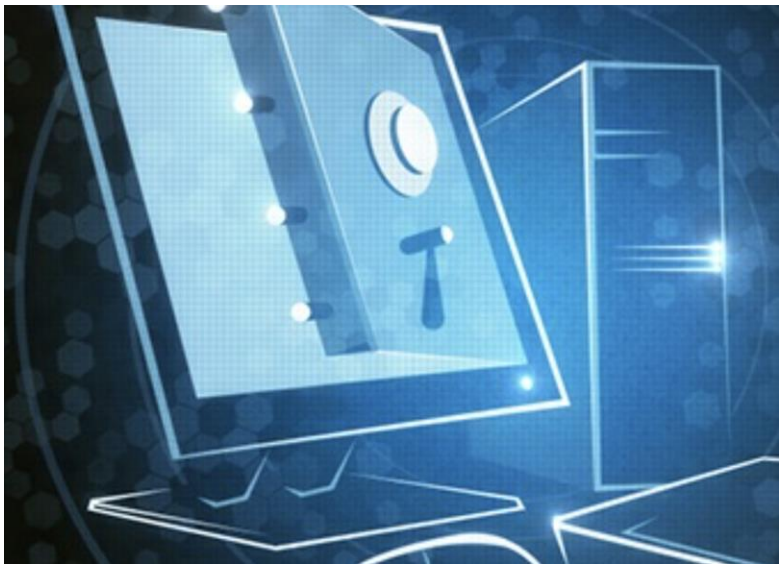


BBC, 2020

customers and was the largest supply-chain breach of all time. this attack also brought third party cyber risk into the spotlight (Chorus, 2021). Secondly, Phishing campaigns by hackers lead to the host computer being compromised by emails delivering emails asking for payments to fake charities, malware delivery, etc. Such attacks nearly doubled in 2020 with the shift to the work from home mode. According to Microsoft's Digital Defense Report (FY2020), phishing mainly occurs through credential phishing and business email compromise. Thirdly, Ransomware is most popular among profit driven and financially motivated attackers. In the UK alone, in the last quarter of 2020, ransomware attacks increased by 80% (Chorus, 2021). For

instance, the highly publicized attack on Australian logistics company, Toll Group saw them being hit by two separate ransomware attacks within three months of one another.

This caused Toll Group to face issues far beyond the costly containment of the attack. They faced serious customer concerns with regards to the identity breach and severe regulatory impacts. Lastly, DDoS attacks overwhelm websites by overburdening them with traffic and thus annihilating its ability to provide any sort of service. This impacts everything from order processing to payments. Record levels were reached in 2020, with such attacks up by 20% YOY (Chorus, 2021). Businesses are affected in a variety of ways through such breaches, there are economic costs, reputational costs, and serious legal ramifications. Theft of funds, information and loss of potential contracts can severely harm the bottom line. The loss of customer confidence translates into a reduction in sales, thus causing a fall in revenue. Data protection and Privacy laws put the burden of protecting such information from falling into the wrong hands on the host organization. A failure to do so invites a tsunami of lawsuits.



FBI, 2019

The international community has been leaning towards an intragovernmental effort to deal with the issue of cybersecurity. The Convention on Cybercrime, widely known as the Budapest Convention, entered into force in 2004 was the first international treaty on crimes committed via the Internet and various computer networks. It dealt with copyright infringements, computer network-related fraud, and child pornography. It also had the power of

interception of various computer networks. It was signed by Canada, Japan, the United States, and South Africa in 2001. As of 2016, Australia, Canada, Dominican Republic, Israel, Japan, Mauritius, Panama, Sri Lanka, and the United States are the non-Council of Europe states that have signed the treaty (Council of Europe, 2016).

Its primary aim, as per its preamble "is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation" (Council of Europe, 2016).

Citations

BBC News. “US Fuel Pipeline ‘Paid Hackers $5m in Ransom.’” *BBC News*, 14 May 2021, www.bbc.com/news/business-57112371.

CDNetworks. “The Industries Most Vulnerable to Cyber Attacks in 2021 –.” *CDNetworks*, 11 Mar. 2021, www.cdnetworks.com/cloud-security-blog/the-5-industries-most-vulnerable-to-cyber-attacks.

Council of Europe. “Full List.” *Treaty Office*, 2016, www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

“Credit Rating Downgrades: Things to Note - Meaningful Minutes.” *Kotak Securities®*, May 2020, www.kotaksecurities.com/ksweb/Meaningful-Minutes/Credit-rating-downgrades-Things-to-note.

“How Cyber Attacks Affected Businesses in 2020.” *Chorus*, 22 Mar. 2021, www.chorus.co/resources/news/how-cyber-attacks-affected-businesses-in-2020.

Morris Worm.” *Federal Bureau of Investigation*, 2 Nov. 2018, www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218.

Tweneboah-Kodua, Samuel, et al. “Impact of Cyberattacks on Stock Performance: A Comparative Study.” *Information & Computer Security*, vol. 26, no. 5, 2018, pp. 637–52. *Crossref*, doi:10.1108/ics-05-2018-0060.


THE EURASIA CENTER