Old Dominion University

# Big Businesses Fight Back!

Clarence Virgil Kimbrell Jr.

CYSE 425W Cyber Strategy and Policy

Professor Lora Pitman

27 February 2022

Protecting critical infrastructure is a necessity for big businesses to operate on a global scale. The majority of people are unaware how protecting critical infrastructure works. It is not as simple as developing an anti-virus software for a big businesses or cooperation's. It is a very in depth layered solution to the rise of hacking. It may be controversial for big businesses or cooperation's to talk about what they are doing to protect critical infrastructure with cyber security insurance because it may defeat the purpose. So, it remains a mystery for its customers and supporters.

Critical infrastructure can be described as absolute essential asset that allows communities and populations to function and allow their economy flow. Examples of such critical infrastructure include things like dams, power lines, and water treatment and so on. Technology has incorporated itself into everything we do, so protecting these valuable assets could save lives.

Terrorist attacks on these assets would be devastating to locals in the area of said attack. This is why big businesses and cooperation's are fighting back and protecting these assets at all costs. The number one main contributor to why protecting critical infrastructure was developed in the United States was following the attack on September 11th, 2001. This introduced a type of attacks, that showed how vulnerable the citizens could potentially be. The policy of protecting critical infrastructure with cyber security insurance is a byproduct of the United States Department of Homeland Security created by George W. Bush[1] on November 25, 2002. After this date it was known that actions were being taken by the government to protect its citizens. These types of attacks on critical infrastructure need to be one of the top priorities for this new

[1] The 43rd President of the United States.

department. The purpose of the policy, protecting critical infrastructure with cyber security insurance, was to increase the safety and wellbeing of its citizens.

Examples of how this policy and strategy have been applied are countless worldwide. The Stuxnet is such an example that could have had devastating consequence it was left untreated. An Iranian nuclear enrichment program[2] fell victim to a cyberattack on critical infrastructure with the Stuxnet virus. It was lurking in the nuclear enrichment software for a year before it was discovered. The causation of such an attack is still up for debate. The leading assumption is an employee launched such an attack by bringing in malware from home. This has supporting evidence because the nuclear enrichment plant has zero access the outside internet which is called an air gap security system. The virus then secured itself within the machinery and operated different patterns of procedure which caused damage to surrounding machinery. Ever since this has occurred there have been many changes to software and malware detection as well as increased physical security within this site only to prevent such an attack again. In the Reuters[3] article section eight, Iranian nuclear enrichment plants have declared that the virus ceases to exist.

The policy fits into national and international strategy because the future of warfare is through cyber-attacks. If one such nation was to create actions disapproved by surrounding nation states they could retaliate through the use of harming critical infrastructure until there was a session of peace. Eliminating sources of power and electricity through cyber-attacks on power grids or nuclear powerplants for example could lead to an early surrender. Examples like this are

[2] A plant like this increases the percent of Uranium-235 for use as fuel in nuclear reactors.
[3] An international news organization.

common so, many wealthy nations have been pushing to protect these assets at all costs because it would have an effect on the big businesses involved.

In conclusion protecting critical infrastructure with cyber security insurance is an absolute essential tool that protect thousand of lives. It is employed by big businesses that work hand in hand with the government regulations within an area. This policy is such a crucial thing for societies to exist, so the direction of it is only going to further improve on existing tools. The emphasis on protecting such assets is only going to increase dramatically in the future.

Sources:

Cantelmi, R., Di Gravio, G. & Patriarca, R. Reviewing qualitative research approaches in the context of critical infrastructure resilience. Environ Syst Decis 41, 341–376 (2021). https://doi.org/10.1007/s10669-020-09795-8

Hanson, Christopher T. "Uranium Enrichment | Nrc.gov." *United States Nuclear Regulatory Commission,* United States Government, 9 Mar. 2021, https://www.nrc.gov/reading-rm/basic-ref/glossary/uranium-enrichment.html.

Hemme, K. (2015). Critical Infrastructure Protection: Maintenance is National Security. *Journal of Strategic Security*, *8*(3), 25–39. http://www.jstor.org/stable/26465242

Janke R., Tryby M.E., Clark R.M. (2014) Protecting Water Supply Critical Infrastructure: An Overview. In: Clark R., Hakim S. (eds) Securing Water and Wastewater Systems. Protecting Critical Infrastructure, vol 2. Springer, Cham. https://doi.org/10.1007/978-3-319-01092-2_2

Limba, Tadas, et al. "Cyber Security Management Model for Critical Infrastructure." *MRU Repository* , Vilnius: Entrepreneurship and Sustainability Center, 2017, 17 Apr. 2017, https://repository.mruni.eu/handle/007/15671.

Mueller, P., & Yadegari, B. (2012). The stuxnet worm. Département des sciences de linformatique, Université de lArizona. Recuperado de: https://www2. cs.arizona. edu/~ collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report. pdf.

Ridge, Tom. “Homeland Security Enterprise.” *Homeland Security Enterprise | Homeland Security*, U.S. Government, 25 Nov. 2002, https://www.dhs.gov/topics/homeland-security-enterprise#:~:text=The%20Department%20of%20Homeland%20Security,the%20United%20States%20against%20terrorism.