MANN GROUP CYBERSECURITY

Cyber War is Upon Us

More bad news was delivered to President Trump in December, with a working group draft report released by the President's National Infrastructure Advisory Council (NIAC). The report begins with these chilling statements:

"escalating cyber risks to America's critical infrastructures present an existential threat to continuity of government, economic stability, social order, and national security."

"U.S. companies find themselves on the front lines of a cyber war they are ill-equipped to win against nation-states intent on disrupting or destroying our critical infrastructure."

"Bold action is needed to prevent the dire consequences of a catastrophic cyber attack on energy, communication, and financial infrastructures."

"The nation is not sufficiently organized to counter the aggressive tactics used by our adversaries to infiltrate, map, deny, disrupt, and destroy sensitive cyber systems in the private sector."

Unlike many things coming from Washington D.C., this is not pure hyperbole. The NIAC provides extensive evidence and a strong argument that urgent action is needed because *"Our window of opportunity to thwart a cyber 9-11 attack before it happens is closing quickly."*

The NIAC report summarizes the 2019 Worldwide Threat Assessment of the U.S. Intelligence Community as follows:

• *China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States.*

• *Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as disrupting an electrical distribution network for at least a few hours—similar to those demonstrated in Ukraine in 2015 and 2016. Moscow is mapping our critical infrastructure with the long-term goal of being able to cause substantial damage.*

• *Iran has been preparing for cyber attacks against the United States and our allies. It is capable of causing localized, temporary disruptive effects—such as disrupting a large company's corporate networks for days to weeks—similar to its data deletion attacks against dozens of Saudi governmental and private-sector networks in late 2016 and early 2017.*

We can add North Korea to the list as well. They attack us with ransomware to the tune of $2B per year. These are all nation states who would prefer the United States did not exist.

Our analysis of the data and report, in conjunction with our tracking of APTs and geopolitics suggest the following:

- The threat is real. Maintaining critical infrastructure has been challenging even without nation state sabotage:
    - California could barely keep its power on when the wind blew in 2019. Can PG&E really be expected to thwart any modern cyber attack? What happens if the state goes dark for 2-3 weeks?
    - Much of Washington State's residents use power and other utilities provided by local government entities, such as the city public works. Realistically, these entities' IT capabilities to defend against concerted attacks are questionable at best, given that large IT-driven enterprises are struggling. What would happen if the Iranians decided to take out a city's power grid and open a dam spillway nearby? The draft report discussed says they have the capability and desire.
- We are living in interesting times, as the saying goes. As we head into the 2020's, we may look back on these days as the calm before the storm. There will be a cyber 9-11; it's not a matter of if, but when, and the impact will be felt far wider than last time.
- Government is taking the right actions, but too slowly. We are likely to see a great deal of acceleration as the threat becomes more widely known by the public, which may be in the wake of a successful and catastrophic attack. Congress will likely overreact following a cyber 9-11 event. The events leading to 9-11 in 1999-2001 can be seen following a similar course in cyberspace in 2017-2019. A cyber Pearl Harbor style sneak attack is not inconceivable.
- Businesses should expect tax incentives and other assistance from government in the future, with the recognition that private industry cannot bear the full cybersecurity burden to protect against nation state cyber attacks and still remain competitive.
- The regulatory environment for internet connected devices will become stricter. For the first time ever, device manufacturers will be required to build security into their products.
- Businesses who prepare for supply chain cyber attacks and make contingency plans will be better equipped to survive than those that don't.
- Large scale cyber attacks by nation states will not be covered by cyberinsurance, which excludes "acts of war". Large security firms, FBI and DHS could be overwhelmed. Small and medium sized businesses will need to be able to fend for themselves in order to survive.
- Government communications often, by coincidence, schedule the delivery of bad or scary news when it can be buried by other stories (e.g. impeachment), or when the public is preoccupied with a holiday (Merry Christmas). The timing suggests there are powerful forces not wanting this publicized.

Mann Group Cybersecurity provides cybersecurity risk assessments and recommendations to small businesses and public entities in Southern Washington at a low cost.

Learn more at www.manngroupit.com

REFERENCES

NIAC Working Group Draft Letter to President Trump, post-dated 12/12/2019:

https://www.cisa.gov/sites/default/files/publications/NIAC-Working-Group-Report-DRAFT-508.pdf

The Hill Story About NIAC Draft Report, 12/10/2019

https://thehill.com/policy/cybersecurity/473682-federal-council-to-trump-cyber-threats-pose-existential-threat-to-the

2019 Worldwide Threat Assessment of the U.S. Intelligence Community

https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

L.A. Times Article on California Blackouts and PG&E

https://www.latimes.com/california/story/2019-10-10/millions-without-power-pge-blackouts-california