BerkeleyLaw
UNIVERSITY OF CALIFORNIA
Berkeley Center for Law and Business

Berkeley Center for Law and Business
University of California, Berkeley
School of Law
Boalt Hall #7200
Berkeley, CA 94720-7220

Ransomware Attacks Grow, Crippling Cities and Businesses

By Gayatri Raghunandan, LL.M. Candidate 2020 | March 3, 2020

Recent years have witnessed several attacks on governments and businesses by Ransomware, a malicious software that can encrypt and control computer systems. Although authorities have not released broad statistics regarding trends, the FBI stated that these attacks are becoming "more targeted, sophisticated, and costly."

Interestingly, before 2019, these attacks were known to target only businesses and individuals. Of late, Ransomware attacks on public-facing institutions is a growing concern. There is a significant threat to public safety, essential utilities, and the backbone of the economy of the city. According to a report by Emsisoft, a security firm, in 2019 Ransomware interrupted 911 services, delayed surgical procedures, and made it tough for emergency response officials to access medical files, scan employee badges, and view outstanding warrants. The report also suggests that in that year, 205,280 organizations submitted files that had been hacked in a Ransomware attack — a forty-one percent increase from the year before.

Slower than average adoption of new technology and a stagnant culture of trivializing cybersecurity are some reasons for the increasing vulnerability of public institutions. The abundance of personally identifiable information (PII) also make city services and hospitals big targets for such criminal activities. This was seen in the recent attack on New Orleans, which led the city to declare a state of emergency. What is worse is that even mitigation strategies such as buying cyber insurance can misfire and have a negative impact. Cyber insurance signifies larger anticipated ransoms. For example, last year, the Florida cities of Lake City and Riviera Beach paid ransoms of about $500,000 and $600,000, respectively. This has led many to emphasize the need to avoid paying ransoms to criminals in the event of an attack. According to data from Coveware, the average payment to release files spiked to $84,116 in the last quarter of 2019, more than double what it was the previous quarter. More so, in December 2019, this figure jumped to $190,946.

Along with entire city governments, several small businesses have suffered tremendous losses from recent Ransomware attacks. Concerns that many small towns in swing states will see more attacks by state-led actors in the wake of the Presidential election in November remain at large. Such attacks on smaller cities are a way to test systems, and motivations for these attacks are wider than mere extortion. However, it can only be hoped that attacks in the past serve as a reminder to enforce greater cybersecurity across public and private facing institutions in the United States.