THE FOODMAN FIRM

MEET YOUR EXPECTATIONS

JUNE 2021

WHO WE ARE

WITH NEARLY **TWENTY YEARS** OF EXPERIENCE HANDLING **COMPLEX, HIGH-STAKES** MATTERS FOR A VARIETY OF CLIENTS - BOTH **INDIVIDUALS** AND **CORPORATIONS**, **DOMESTIC** AND **INTERNATIONAL** - **THE FOODMAN FIRM CONSISTENTLY PRODUCES** VALUE-DRIVEN **RESULTS** FOR OUR CLIENTS, WITH AN EMPHASIS ON **QUALITY OVER QUANTITY.**

OUR PRIMARY FOCUS AT **THE FOODMAN FIRM** IS TO PROVIDE OUR CLIENTS WITH THE MOST EFFECTIVE COUNSEL, **AND TO FOSTER LONG-TERM RELATIONSHIPS THAT OUR CLIENTS CAN DEPEND ON.**

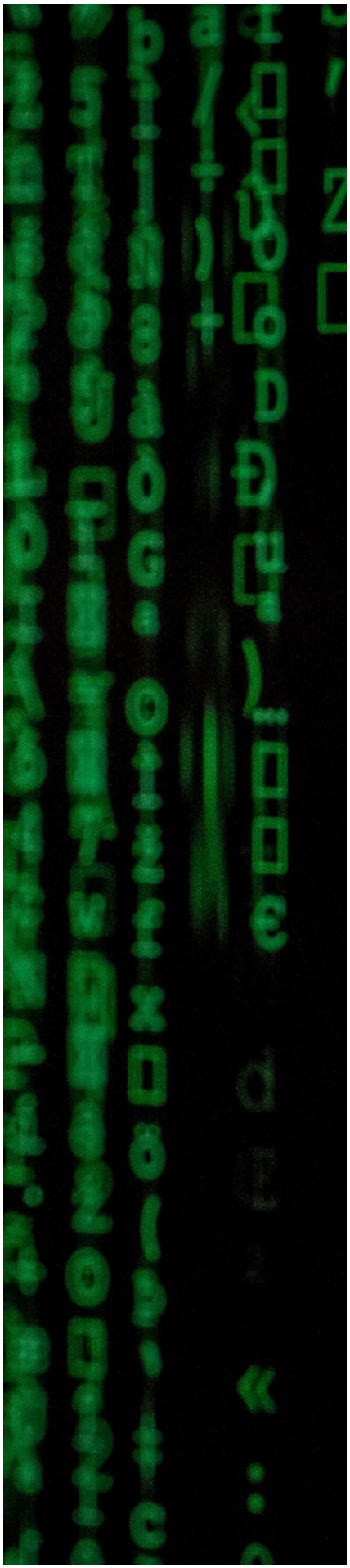
THE FOODMAN FIRM TAILORS ITS INNOVATIVE FEE STRATEGIES TO MEET THE INDIVIDUAL NEEDS OF EACH CLIENT.

TABLE OF CONTENTS

THE COLONIAL PIPELINE CYBER ATTACK

The May 7, 2021, ransomware attack on the Colonial Pipeline was a wake-up call to the United States and worldwide regarding the massive implications of such an attack.

Colonial Pipeline Co., ("Colonial") operates a 5,500-mile pipeline that delivers almost half of the total gasoline supply for the east coast of the United States. The breach, which shut down the pipeline, has been described as the largest cyber-attack on an infrastructure oil company.

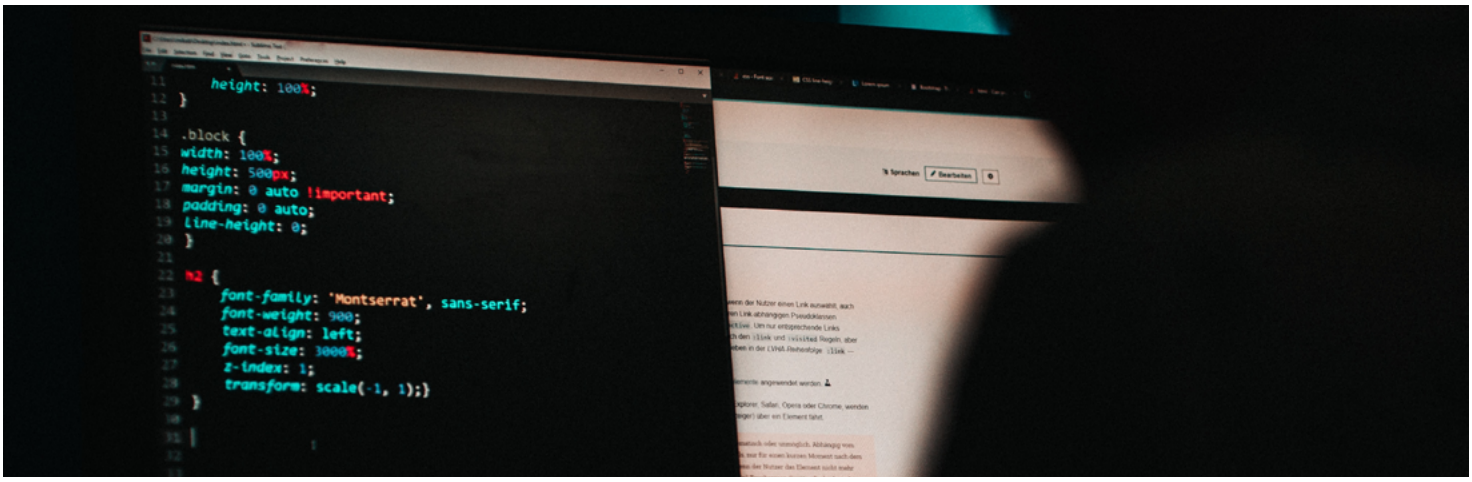


Indeed, it caused an immediate surge in gas prices, and long lines at gas stations on the east coast.

Ransomware is designed to paralyze the target's computer systems until a certain sum of money, a ransom, is paid to the attackers, usually in cryptocurrency. The volume of ransomware attacks has drastically increased, perhaps fueled by the surge in the value of cryptocurrency, or because of the increased reliance on interconnected computer systems by society, including companies integral to infrastructure. Indeed, infrastructure is a prime target for cybercriminals because of the physical implications of the attacks, namely, the impact on basic daily needs because any amount of time holding the system hostage can be extremely valuable.

Imagine, a cybercriminal holding an electrical or water supply computer system hostage – it can be an immediately destabilizing event from a health and safety standpoint.

Thus, companies like Colonial often succumb to the demands and pay the ransom to regain control of their systems instead of suffering the repercussions of an extensive shutdown. To be sure, it has been reported that Colonial paid nearly $5 million to a well-known hacker group, Darkside, to regain control of their systems. While the Federal Government



advises that companies should not pay a ransom in such an attack, similar to its view on terrorism and kidnapping, that view is shortsighted because the result in a case like Colonial is increased pricing and limitations to tens of millions of people on a necessary product, which has far-reaching economic impacts far in excess of $5 million.

The economic impacts for Colonial will exceed the $5 million paid to the hackers. The first of potentially many class action lawsuits has already been filed in a Georgia court alleging negligence surrounding Colonial's response to the cyberattack and the following shutdown.

The plaintiff in the suit is seeking damages from Colonial, primarily in response to the increase in gas prices for millions of Americans along the east coast.

The plaintiff in the suit is seeking damages from Colonial, primarily in response to the increase in gas prices for millions of Americans along the east coast. The lawsuit mentions other cyberattacks on infrastructure like the ones on the Ukrainian power grid in 2015 and on SolarWinds in 2020 as evidence that Colonial should have been aware of potentially being targeted by hackers and therefore should have had measures in place to prevent these attacks.

The potential implications of future lawsuits may be enough of a threat for similar infrastructure companies to begin to bolster their cybersecurity moving forward, independent of government regulation.

In that regard, in its reactive response to this attack, the Administration is planning to adopt mandatory cybersecurity requirements for pipelines, and it issued a feckless Executive Order on cybersecurity. Under a forthcoming security directive, pipeline operators would be required to immediately report cyberattacks to the Department of Homeland Security, which Colonial reportedly did report to law enforcement at the time of the attack before the issuance of a security order and undoubtedly any rational corporation would do so under the circumstances without prompting. There will also be mandates for how pipeline companies will be required to protect their systems and data in the future.

These are important steps that many will argue should have already been in place for all infrastructure systems as important as gas pipelines, and noticeably absent from the Administration's response to the Colonial attack. Accordingly, this is something that should be taken up in a bipartisan manner by Congress as ransomware attacks on infrastructure companies are a national security risk, and there is no sign that the reliance on computer systems will slow down, which without proper security, the number of cyberattacks will certainly continue to increase.

FLORIDA LEGISLATIVE UPDATE

Out of the recent controversies surrounding bans of elected officials and communication platforms by Facebook, Apple, and Twitter, the Florida legislature passed Senate Bill 7072 to regulate social media companies. In that regard, on May 24, 2021, Florida's Governor, Ron DeSantis, signed the Senate Bill "to hold Big Tech accountable by driving transparency and safeguarding Floridians' ability to access and participate in online platforms." The law creates three new statutes describing regulation for social media companies including, prohibiting social media platforms from knowingly deplatforming a political candidate or journalistic enterprise because of their publications, authorizing social media platforms to provide free advertising for political candidates under certain conditions, restricting the use of algorithms and "shadow banning" for content filtering, and providing fines for those violations.

Deplatforming is defined as any action by a social media company to permanently remove or ban a user from the platform for more than 14 days. A shadow ban occurs when a user's content is limited or eliminated from view from other users of the social media platform, usually without the banned user's knowledge. The controversial new law also allows social media users to sue companies who violate these laws for monetary damages. Notably exempted from this new law are theme-park operators in Florida.

It is expected that social media companies will bring court challenges based on 1st Amendment arguments, the same arguments made by those banned by them. In particular, the companies will argue that internal moderation practices are within their own 1st Amendment rights, which is a largely unsettled area of law. However, it is an area of law that needs to be settled with urgency because large numbers of Americans are of the view that social media companies are engaged in stifling free speech by banning certain individuals and platforms. Those who oppose these practices by social media companies believe that the companies' 1st Amendment rights should not supersede those of the users on their platforms, and and that moderation actions by social media companies should have some level of transparency and regulation.

Balancing these two opposing viewpoints will be no easy task for a Court, and the implications of the potential success or failure of this law will undoubtedly have an impact for years to come on similar legislation of other states or the federal government.

THE FOODMAN FIRM

Call us today at **(305) 201-3663** or visit our **WEBSITE** to schedule a consultation to discuss your business's needs and how The Foodman Firm can assist you!

If you want to sign up for our newsletter, please **CLICK HERE**, and follow us on **LinkedIn**