Cyberattacks Threaten Business, Industry, and Infrastructure - This Week's Victims Include a Pipeline, Major Municipalities, and a Tribal Government

By: R. Trent Shores and Tom C. Vincent, II

Colonial leader and Founding Father Benjamin Franklin advised that an ounce of prevention was worth a pound of cure. One must wonder to what extent Colonial Pipeline or any of the other ransomware victims in the news had invested in cybersecurity prevention. Today's world functions in large part due to interconnected digital networks where information, currency, and other data are merely a hack away for cybercriminals, cyberterrorists, and enemy foreign states. With the onslaught of recent cyberattacks, it is clear that any individual, government or business must be proactive in building up its defenses against cyber incursions and preparing for the aftermath if and when there is a breach.

American ingenuity drives world markets and inspires advances in science and technology. Nowhere is that more true than in the energy industry where American innovation, born out of our free-market system and democratic values, is the envy of the world. That makes American companies and institutions valuable targets for cyberattacks and espionage. It also puts a target on American cities and states where those companies are based. Now, more than ever, it is essential that our systems and data are both secured and preemptively protected – both in terms of managing competitive business advantage and in protecting the private information of customers, clients, and employees. Neither a remnant of the by-gone Cold War era nor a creative plot of a sci-fi movie, cyber-espionage is a real and increasingly frequent threat to all Americans.

Cyberattacks Today – Fact, Not Fiction

Attacks are taking place in governments, businesses in every industry, and in the labs of academia. From coast to coast, hackers have infiltrated nearly every sector of our economy and government. Rural businesses and industries are no more immune to cyberattacks than their counterparts in densely populated areas. We've learned that the hard way in America's heartland where major energy companies, aviation and aerospace industries, and extensive agricultural research and development thrive.

While the attack on Colonial Pipeline has dominated national headlines, we need not look beyond the borders of Oklahoma to note significant cyberattacks which impacted two governmental entities: the City of Tulsa (reminiscent of the 2018 attack on Atlanta) and the Seminole Nation of Oklahoma. The City of Tulsa and the Seminole Nation were hit with ransomware attacks similar to that used against Colonial Pipeline. As described by the Federal

Bureau of Investigation, "ransomware" is "a type of malicious software or malware that prevents you from accessing your computer files, systems or networks and demands you pay a ransom for their return." Let's also not forget the Russian government's hack of SolarWind's proprietary software used by top American government agencies and tech firms. Nor should we turn a blind eye to the Chinese government's suspected in role in hacks of U.S. government databases that compromised more than four million federal workers' personal information.

The consequences of such an attack can be disastrous and costly for not only governments and businesses but also individual Americans. As America's enemies pursue their quest for global dominance, cyberattacks such as these should serve as a wake-up call to the United States – and all of the governments, municipalities, businesses, and individuals in it.

Respond Quickly and Completely to Any Attack

In order to confront and counteract the hardball tactics of enemy states and their leagues of hackers, the United States government must be aggressive in identifying and prosecuting those engaged in trade secret theft, hacking, and economic espionage. Any company, organization or other entity who has suffered a loss from cyber or insider threats should report the breach to their local FBI field office. If you say something, they can do something.

In the meantime, private sector business leaders and cybersecurity experts must step up their efforts to help protect America's critical infrastructure against external threats, including foreign direct investment, supply chain threats, and foreign agents seeking to influence the American public and policymakers. Better yet, don't wait until you are a victim to think about cybersecurity measures.

For example, if you are unfamiliar with terms such as phishing, spoofing, credential stuffing, key loggers, red teaming, and penetration exercises, then your organization may be vulnerable to cyberattack. If you do not have a cybersecurity crisis communications plan in place, it's imperative to develop one now - not after the breach has occurred. Preparation and prevention means providing continuous cybersecurity training to employees, while also engaging in monitoring, oversight, and compliance reviews for any third-party vendors to ensure those third parties are aware of their own particular responsibilities and are fulfilling them as required by statute, regulation or contract. Be proactive and invest in that ounce of prevention.

Before An Incident Occurs - Prepare

To best protect the interests and information subject to attack, governments, businesses, and industries should, at a minimum, be aware of both i) the types of information that they collect and ii) the various requirements for cybersecurity that are applicable to them. For most of these organizations, the first (and sometimes last) line of defense is their employees – information technology departments may be able to install firewalls, but they can't prevent an employee from "clicking that link" (at best) or preventing active theft (at worst – see below):

One Chinese national, Hongjin-Tan, was convicted through the work of the United States Attorney's Office for the Northern District of Oklahoma, and sentenced to serve time in federal prison for stealing trade secrets from a major petroleum company in Bartlesville, Oklahoma. While employed as an associate scientist for Philips 66, Hongjin Tan stole information related to next generation battery technologies for stationary energy storage. This proprietary information was estimated to be worth more than $1 billion. The spy surreptitiously downloaded and copied critical files from the company databases in order to replicate the technology at his newly acquired position at a Chinese battery technology company.

This theft of trade secrets was not an isolated incident. According to FBI Director Christopher Wray, the FBI was investigating more than 2,000 possible instances of Chinese trade secret theft through all 56 FBI field offices across the country in 2020. For example, a Chinese citizen was convicted in federal court in Houston, Texas, for conspiring to steal from an American competitor deepwater trade secrets related to the manufacture of syntactic foam, a buoyancy material that has off-shore drilling and military applications. Last year in New York, a federal grand jury returned a superseding indictment of Huawei - a prominent Chinese telecommunications conglomerate, and its U.S. subsidiaries - with a racketeering conspiracy, conspiracy to steal trade secrets, and conspiracy to commit wire fraud. Huawei and its coconspirators are alleged to have agreed to misappropriate intellectual property from at least six U.S. companies in order to grow and expand operations. In 2019, a federal grand jury in western Washington also charged Huawei with conspiring to steal trade secrets from T-Mobile, alleging among other things that Huawei offered bonuses to employees who succeeded in stealing confidential information from other companies. More recently, in 2020, two Chinese hackers were charged with stealing and attempting to steal terabytes of data, including coronavirus research, trade secrets, intellectual property, and other valuable business information.

To ensure employees don't inadvertently assist attackers, employees should be aware of the three categories of rules – laws/regulations, policies, and procedures – and be given ways to follow them. Supplementing these should be appropriate mechanisms and incentives to motivate employees to put this knowledge to best use within the company and act to support the company's cybersecurity efforts. As discussed above, knowledge of what to do for cybersecurity is not enough - employees must understand that they have the power to impact cybersecurity at the company and the right and responsibility to do so. Once employees know the rules, they need to be able to follow them. Just as with education, empowerment of employees should be provided at multiple levels to allow them the greatest opportunity to prevent attacks both from without and within.

Checklist of Employee Empowerment for Cybersecurity

1. **Establish, at hire, the expectations of particular employee responsibility and behavior regarding cybersecurity.**
   - Addressed in job description
   - Reinforced by hiring manager and Human Resources
2. **Train employees on the general laws, regulations, and requirements the company is subject to.**
   - Include applicable federal and state laws and particular contractual commitments.
3. **Adopt specific policies and procedures with respect to cybersecurity.**
   - Overall cybersecurity policy to set the general direction and overall tone for the company's priorities and the individual actions of its employees
   - Targeted departmental policies to bring the company's goals into focus for the particular responsibilities of employees
   - Procedures to give employees guidance to fulfill both company policies and their specific responsibilities
4. **Communicate the consequences of employee action or inaction.**
   - At the company-wide level - the company may inform employees as to cybersecurity efforts, and also empower them to take action, but also follows up to verify that appropriate action is taken by its employees
   - At the employee level, identify expected fulfilment of that responsibility through goals established during performance reviews
5. **Provide responsibilities for the employee within the company to raise cybersecurity issues.**
   - Appropriate reporting structure to provide an additional sense of ability and responsibility to the employee to raise and report on issues

The collective response from America's private and public sectors will send a clear message to the any would-be enemy states and cybercriminals. Thus, it is imperative at this pivotal time that our public and private sectors stand together, unified, to guard the long-term security and prosperity of this country and everyone in it.

Trent Shores is a Shareholder at GableGotwals and is a former United States Attorney and National Security Cyber Coordinator for the Tulsa-based U.S. Attorney's Office in the Northern District of Oklahoma. Tom Vincent, CRCM, CIPP/US is a Shareholder at GableGotwals and is the Firm's Cybersecurity and Data Privacy Practice Group Lead.