



ARMADA

NAVIGATING PREPAREDNESS & PROTECTION

It's no surprise that in today's digital world, Cybersecurity is one of the most important challenges we face as a nation. Criminals, terrorists, and countries who wish to do us harm have all realized that attacking us online is often easier than attacking us in person. As more and more sensitive data is stored online, the consequences of those attacks grow more significant each year. We have built trust for the "secure" and "hacker-protected" guarantees that are provided with business technology in which we confide in, but is it really a 'guarantee' that our information will never be disclosed to additional parties? Recent events exemplify that effective communication and preparation are possible solutions to surviving cyberattacks.



According to the Los Angeles Times, on February 5 a cybersecurity assault was placed Hollywood Presbyterian Medical Center, when hackers using malware infected the institution's computers, preventing hospital staff from being able to communicate from those devices. The hacker demanded \$17,000 and would only release access when the money was paid. The hospital's Chief Executive, Allen Stefanek, claims the hospital "acted in the best interest of restoring operations" by paying the ransom. While the good news is that no patient care or hospital records were compromised, Hollywood Presbyterian Medical Center unfortunately did not communicate and alert authorities until after the ransom was paid. While it is rare, this is not the first medical institution that has been a target for cyberattacks and it most likely will not be the last. It's very possible that the hospital could have saved itself thousands of dollars if a response plan incorporating effective communication was utilized.

In light of the increased national awareness from cyberattacks in the earlier part of the decade, Central Ohio stakeholders had determined there was a gap in cybersecurity preparedness between private and public sector partners and it was time to implement a plan to prepare for, respond to, and recover from cyber threats. Beginning in October of 2014, ARMADA led Central Ohio Stakeholders in a nearly year-long planning effort that involved more than 40 participants from across the region, including the integration of key public and private sector partners. These stakeholders met on a monthly basis to discuss current events, best practices and increase overall communication in an effort to prevent situations like the one that occurred in Los Angeles.



It is critical to recognize cybersecurity as an ongoing threat which, as technological intelligence strengthens, will only continue in severity to pose harm on ourselves, businesses, government agencies and institutions.

For more information on how you can successfully prepare for, respond to and recover from cybersecurity threats, contact ARMADA at (614) 437-9700.