WANNACRY AFTERMATH

By Derek Laczniak, Director of Cyber Practice, M3 Insurance

As we continue to look forward as to what the future of data security and cyber liability holds, it is critical that we do not forget the present. A strain of ransomware known as "wannacry" struck 100,000 organizations in at least 150 countries since first appearing last week. Fortunately, many of the organizations were outside of the United States and the commonplace IT practice of updating and patching systems on a regular basis prevented the infection from hitting countless organizations.

Given the nature of the "wannacry" program, it is possible to track how much ransom the cyber criminals behind it have actually collected. Despite the number of organizations affected, interestingly, the total ransom collected at last count was only around $35,000. However, the downtime costs that each infected organization experienced are not included in this figure. Those numbers will not be captured in the ransom demand, but rather in insurance claims or sunk costs for those that fell victim.

Although the "wannacry" outbreak was frightening, it could have been much worse. The virus was not designed to penetrate internal networks, but only the local drives of the machines it hit. That means that only the physical computers were victims of this crime, and not the entire network of an organization. Also, as private information was not stolen or compromised, victims of this particular attack were saved the costs involved with massive reporting and disclosure of the breach.

These types of viruses evolve at a faster pace than the solutions to fix them. This incident serves as a reminder of the cyber landscape we live in and how it will continue to evolve, requiring our utmost attention and respect.