Dickie McCamey
ATTORNEYS AT LAW

6/16/2017 | Articles

An Increase in Ransomware Attacks — Are You Prepared for the Inevitable?

On May 12, 2017, a ransomware cryptoworm (now referred to as the “WannaCry” worm) was unleashed worldwide on systems utilizing Microsoft Windows operating systems. The effects were ubiquitous, with governmental and private systems located in over 150 counties compromised in the attack. By encrypting data on the infected systems, the attackers were able to demand ransom payments in Bitcoin in exchange for the encryption key to release of the systems. Although the attack garnered substantial media attention, indications are that the attack itself was not expensive for the insurance industry. Nevertheless, the *Financial Times* has reported that so-called “ransomware” has become “the fastest growing cause of cyber insurance claims.” The ransomware attack is not new — its prevalence, however, has increased.

Organizations of all sizes are increasingly concerned about their liability in the event that their enterprises suffer any type of cyber-attack. The law struggles to adapt to the rapidly evolving technology (and any attendant standard of care) and the cyber-crime that follows; in fact, there is a dearth of case law addressing claims related to “ransomware.” Interestingly, most federal class actions associated with data breaches involve stolen personal or sensitive data. These claims often do not involve actual misuse of data or financial loss, only the alleged increased risk of future harm to the person whose data was stolen.

Thus far, courts have been reluctant to impose liability on organizations for an increased risk of future harm. Courts have considered, however, more than 50 different theories of recovery in data breach cases. Most commonly, claims are predicated on a failure to properly secure data via claims of negligence, invasion of privacy, breach of contract, requests for equitable relief, and violation of state consumer protection and notification laws. Negligence-based theories have been panned by courts adhering to the “economic loss” doctrine, which requires physical injury to a person or property for liability to attach. Consumers are on stronger ground when asserting claims based on state consumer protection statutes or statutory data breach notification laws. An interesting and developing avenue of recovery are claims for equitable relief, by which claimants argue that fairness dictates that the custodian of their personal data answer for breaches of privacy even though the custodian may not have been negligent.

Imposing liability on large organizations will create a precedent that could be overly burdensome for small and mid-sized organizations. Thus, courts have treaded lightly when considering these claims, especially negligence-based claims that would impose a duty on small organizations to utilize the expensive and sophisticated prophylactic security systems that large organizations could afford (and still without the guarantee that a company’s data would be secure from attack). Regardless, plaintiffs continue to seek viable theories of recovery when they fall victim to a cyber-attack or other data breach.

With the increased occurrence of ransomware attacks and the absence of any guarantee that your organization will not fall prey to a breach, having an experienced legal team in place can reduce your risk and ultimate liability.

If you have any questions regarding the information outlined above or any other inquiries, please feel free to contact us.

Christopher J. Watson
412-392-5678
cwatson@dmclaw.com