LW Consulting, Inc

Would Your Business Survive RANSOMWARE

Ransomware is a type of malicious software that threatens to publish the victim's personal and medical data or perpetually block access to it unless a ransom is paid. While some simple ransomwares may lock an entity's operating systems, making it difficult for a knowledgeable person to reverse, more advanced malware utilizes a technique called cryptoviral extortion. It encrypts the entity's files, making them inaccessible, all while demanding a ransom payment prior to decryption.

THE EFFECTS OF RANSOMWARE SO FAR

The Health and Human Services (HHS) Office of Information Security and Health Sector Cybersecurity Coordination Center (HC3) presented Ransomware data on June 3, 2021. HC3 reports tracking ransomware incidents worldwide within healthcare and **nearly 60% of the incidents have impacted the United States health sector.** The top victims in 2021, within the U.S., as of May 25, 2021 were Health or Medical Clinics accounting for over eighteen ransomware incidents occurring in California, Texas, Georgia, Illinois, and Louisiana. The U.S. incidents **resulted in entity data leaking in at least 72% of the incidents.** HC3 reported, **the average ransomware payment is $131,000,** which does not account for staff downtime, device upgrade costs, network cost, lost opportunities, or forensic consulting costs to rectify the incident.

ALL PRACTICES AT RISK

On June 15, 2021, Chiropractic Economics published an article titled, "Ransomware removal and the most common health care cyberattack." This article appears to mirror the trends reported by HC3, noting a shift to Health or Medical Clinics becoming the primary ransomware targets. Described here are a few of the author's key highlights from Chiropractic Economics.

CRIPPLING COSTS

The national average cost to mitigate ransomware is $158,000 with smaller practices averaging $90,000. This includes fines and penalties.

TARGETED PROVIDERS

Small, specialty providers are increasing targets. For example, 2-4 chiropractic offices are hit by ransomware per month, posing economic threats resulting in a possible business shutdown. 89% of cyberattacks are now ransomware.

"WILLFUL" FAILURE

Practice owners are required to ensure the Confidentiality, Integrity, and Access of data as part of HIPAA Security, maintain Business Associate Agreements, and provide staff training regarding breach reporting. Failing to perform a Security Risk Assessment (SRA) on your operating systems could be viewed as "willful neglect" resulting in higher HIPAA fines and penalties.

HOW TO PROTECT YOURSELF

Is the price of not conducting a SRA now worth losing your business? Now is the time to budget and plan your SRA in 2022. Not sure if you are protected,? Let LW Consulting, Inc.'s HIPAA security consultants assist you with the decisions. LWCI offers the **HIPAA SP3: Security Policies and Procedures Package** which can be found on our LWCI Learning Center, or our experts can set up a time to discuss your SRA and HIPAA Security and Penetration Testing needs.

To learn more about how LW Consulting, Inc. (LWCI) can assist, contact Deborah Alexander, Director, CHC, CHPC, PMP, DPT, MED, STC, CSCS at DAlexander@lw-consult.com or by phone at (215) 907-8740.