Howard University is the Latest Educational Institution Hit with Ransomware Attack

Earlier this month, on September 3, Howard University's technology team noticed "unusual activity" on the school's network. To investigate the problem, school officials shut down the entire network, upon which they uncovered a ransomware attack. School officials have been subsequently working closely with the FBI and DC city government to determine the extent of the hack. At this time, they believe no personal information of the students and faculty has been accessed or exfiltrated. However, the university has been virtually offline and will begin to resume online courses effective September 13.

The ransomware attack on Howard University is emblematic of the current cyber risks facing educational institutions. The education sector is one of the leading industries facing the highest overall cost to recover from a ransomware attack. Experts estimate that the combined downtime, people time, device cost, network cost, lost opportunity and ransom paid by educational institutions has skyrocketed their total average cost in responding to a ransomware attack to $2.73 million. This cost is 48% above the global average.

POPULAR TARGETS

Ransomware criminals view educational institutions as easy, soft targets: educational institutions typically have expansive and disparate technology projects that can remain unpatched without centralized oversight. As such, educational institutions and especially colleges and universities, are popular targets for ransomware attacks.

Famous for budget issues, hackers know universities are lucrative targets as universities appear willing to pay huge amounts of money to pay ransoms when forced. Experts have reported that 29 American educational institutions have been hit with ransomware attacks in 2021. In the second and third quarters of 2021, there was a 388% increase in successful ransomware attacks on the education sector. Howard University joins a growing list of universities that have experienced ransomware attacks, including University of California, Stanford University and Michigan State University.

Compare these numbers to 2020, in which there were 32 ransomware attacks against universities. For instance, the University of Utah and University of California, San Francisco both admitted to paying ransoms following the 2020 cyber-attacks.

MORE RANSOMS, MORE DEMANDS

Cybercriminals are employing what is known as a double extortion tactic against educational institutions. Not only are the cybercriminals demanding a ransom after encrypting data and hijacking victim institutions' environments, but they are also extricating student and faculty data. Cybercriminals are now demanding an additional ransom not to publicly release that information.

Cybersecurity and IT experts believe the best way to avoid paying ransoms is to maintain encrypted backups of all data. They should regularly test their usage and be stored offline as cybercriminals look for and delete backup information. Schools and universities could avoid paying ransoms if the data remains in their hands.

In addition, cyber response plans should be developed. The response plans include training staff in the procedures and conducting drills to ensure a smooth response in the event of a real attack. Therefore, the best way to prevent these attacks is to be prepared ahead of time.

For more information, please contact Matthew Plotkin at matthew.plotkin@nfp.com.