Drexel Hamilton
A Service-Disabled Veteran Owned & Operated Business

Outside the Wire
Drexel Hamilton on Recent Cyber-attacks

In the middle of the COVID-19 pandemic, many school districts have opted for online learning. While online learning can keep students, teachers, and staff safe and social distanced during a pandemic, it throws the door wide open to security concerns in the cyber domain.

While the summer's Twitter hack made news because it involved a host of well-known politicians and celebrities whose accounts were compromised, others have occurred of equal importance. The recent successful ransomware attack on Clark County School District in Las Vegas adds to a long list of municipalities that have been hacked. These attacks can be costly not only in the near term, but they can have long term implications on the credit quality of an issuer.

What is ransomware?

In the analog days, criminals might have sent a paper note with a bunch of cut out letters. But the cyber version of this is for cyber criminals to lock people out of their own networks. The subsequent demands call for a payment in bitcoin. No more cash filled briefcases. Cyber thieves want the real digital thing and bitcoin is the preferred payment. In many cases, the “or else” part of the ransomware attack is that data to include personal information like social security numbers will be released.

In the case of Clark County, school district officials stood toe to toe with the unseen cyber sleuths and refused to acquiesce. The hackers then published documents with private information on students, teachers, and employees.

The Wall Street Journal reported that in many cases school districts will decide to pay the ransom and move on. They point out that Sheldon Independent School District in Houston, Texas is an example of a district that decided to pay the bitcoin ransom demanded. They did so to the tune of $206,931 in bitcoin. Also, cited in the article is a cyber-negotiating firm called Coveware, which reported that ransomware payments averaged $178,254 for the end of the 2nd quarter in June.

From a geopolitical standpoint, we understand a few things to be true. First, hackers can range from non- state to state actors. The danger of state sponsored hacking is real and costly to American businesses and municipalities. Second, as the United States imposes sanctions on countries like Iran and North Korea, we understand that the threat of these hacks will only increase. Furthermore, they will specifically look for "soft" targets, which means schools and cities that don't have their own offensive cyber capabilities.

While we do not know whether Clark County or Sheldon Independent School District were targeted by a state actor, we know that other municipalities have been.

In March of 2018, it was revealed that the city of Atlanta had been hacked. The hackers demanded $51,000 in bitcoin. According to Reuters, the hack cost the city around $9.5 million. The Department of Justice indicted two Iranian hackers as the primary culprits.

While the Atlanta case made a splash as the largest American city to be successfully besieged by hackers, the city of Baltimore followed as the next major target in May 2019. In that case, hackers demanded $76,000 in bitcoin. Baltimore declined to pay. The economic damage totaled around $18 million.

How does this happen?

In many cases, the hack involves a phishing e-mail. These can be incredibly deceptive. Hackers use e-mails that appear to be from real sources like friends, co-workers, managers or even someone from the IT staff. They might ask the target to click on a link or open an attachment. This becomes the equivalent to unlocking the door. The victim can be asked to provide information that can allow the hacker to gain credentials that might give them access inside specific networks. From there, weeks can go by as hackers gain sensitive information and install sophisticated software that will ultimately be used to set up the ransomware.

What are the solutions?

First and foremost, employee training is important. Even employees at big tech companies like Twitter can be duped by a hacker. Nevertheless, training to recognize possible phishing scams is a strong start.

Second, we buy insurance for our cars and homes. But many municipalities do not have cyber security insurance. If they do not, this could be a costly mistake. As more services go online, it only increases the demand to be properly protected. No network is off limits. From public libraries to transportation systems, any public service with an Internet connection has a target on its back.

Even corporations designed to help municipalities improve their software can be victims. On September 24, Tyler Technologies (NYSE: TYL), a company with over $1billion in revenue, was hit with a ransomware attack. Tyler Technologies provides software for municipalities. The website BleepingComputer reported that the hackers used RansomExx malware, which is believed to be tied to Russian sources. Although Tyler Technologies claims to have contained the threat, paid for decryption and moved on (the stock recently hit all-time highs), the website Cyber Security Hub claims that clients are still reporting suspicious activity to include “unauthorized login attempts and unauthorized software installments.”

Conclusion

Last year, several Drexel Hamilton employees read and shared a book titled *The Fifth Domain: Defending our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. The book was co-authored by Richard A. Clarke, former presidential advisor on intelligence and counterterrorism to Presidents Ronald Reagan, George H.W. Bush, and Bill Clinton, along with Robert K. Knake, who is a senior fellow at the Council on Foreign Relations. One of the book’s main themes is that governments, corporations, and individuals need to take seriously the cyber battlefield and build stronger defensive capabilities. While the U.S. has a well-functioning federalist system that largely decentralizes decision making to states and local governments, this system causes a lack of national coordination in terms of cyber defense. Therefore, municipalities and companies function independently when it comes to cyber risks. With that being the case and considering the strength of possible state-sponsored attackers, leaders must be pro-active in building a robust defensive capability.

Disclaimer: The information and statistical data contained herein have been obtained from sources that Drexel Hamilton, LLC (“Drexel”) believes are reliable, but Drexel makes no representation or warranty as to the accuracy or completeness of any such information or data and expressly disclaims any and all liability relating to or resulting from your use of these materials. The information and data contained herein are current only as of the date(s) indicated, and Drexel has no intention, obligation, or duty to update these materials after such date(s). These materials do not constitute an offer to sell or the solicitation of an offer to buy any securities.