Getting Away from the Ransomware Triple Threat

Your own district could easily be the next victim of a cyber-attack. What are you doing about it?

James Morrison
Distinguished Technologist, Cyber Security
Hewlett Packard Enterprise

EVEN THOUGH IT'S NOW A SIMPLE MATTER to go online and learn how to launch a cyber-attack and buy the tools to do so for just a few dollars, ransomware has become a more complicated process, involving triple extortion. Originally, the idea was that the bad guys would get into your computer system, encrypt your data and tell you that in order to get the data back, you'd have to pay ***x*** bitcoins. That was pretty direct; you either paid the money and hoped they'd give you your data or you had backups, because a good backup policy would prevent an attack from imposing any lasting damage.

So the criminals revised their approach. They turned around and said, "OK, we've encrypted your data. Pay this amount to get it back. And by the way, we also stole your data. If you want to prevent this data from being made public, you will pay the same amount of ransom, and this is the deadline." A recent example was JBS, the meatpacking plant that was hit by a cyber-attack. The company had backups and recovered its data without paying for the encryption key – but it paid $11 million dollars, hoping to prevent the stolen data from being exposed.

Now there's a third level. The criminals will threaten to post your organization's name on a shame website that says you were a target of their theft. They'll also contact people – students, staff, parents – victimized by the ransomware, encouraging them to stop doing business with you. If it's K-12, that kind of outreach would become fodder for grim news headlines, putting a major dent in the school district's reputation and leading to panicked decision-making among administrators and school boards.

Plus, there's the expense of mopping up the damage done by a data breach. Although schools don't always realize that data breach laws apply to them, they certainly do. And because ransomware is now accompanied by a threatened data breach, by law, districts are expected to disclose the break-in and notify those who could have been affected, even if they don't think they've lost any data. Any district leader who thinks a cybersecurity insurance policy will save the day (and pay the bills) is being short-sighted. Increasingly, insurance companies are starting to push back on giving ransomware insurance.

Where does that leave you? I suggest you start by covering the basics of cybersecurity. These are four fundamental steps that will minimize the risks of suffering a cyber-attack and mitigate the damage if or when your district is hit.

4 Steps to Safety

First, identify your risks. That means having a penetration test done, preferably by an outside entity. For example, in my state, Texas, schools can arrange that through a dedicated agency, the Department of Information Resources, and the state will supplement the cost. Similarly, the regional consortiums and other education organizations you belong to may offer the same services. This will provide a baseline for understanding where your major risks lie.

Second, set up a solid data classification. When I was in the military, classification of information was common – secret, top-secret and so on. But districts too need to put data into their proper siloes. And then based upon those classifications, you'd designate the level of data protection. As an example, the data that's considered sensitive because it contains personally identifiable information should always be encrypted. Higher education is accustomed to forming data governance councils to tackle this work; the practice is less common in K-12, but it's an effective way to convene the various stakeholders and sort out the details.

Along with that data classification, it's important to think about what data you really need to store in online repositories and how long you need to keep it. Districts often keep too much data or hold onto it longer than they need to. And that's a problem. Even years-old data has value to somebody on the dark web.

Third, segment access rights. System administrator rights should be given out to the fewest number of people possible. The problem I've seen in K-12 is often that the smallest districts will have tiny or even part-time IT teams, and so they'll do what's easiest and what's convenient, but not necessarily what's most secure. Striking the right balance among ease-of-use, access and security will always be something that districts struggle with.

Fourth, choose providers that can help you lessen the work burden. For example, HPE's GreenLake Central provides a front end that operates between the district and its various cloud providers – both the public clouds operated by Google, Amazon and Microsoft and the private clouds running virtually in your own data center or externally. GreenLake is built on the world's most secure servers. We are responsible for securing all the virtual machines, the containers, the hypervisors and everything else that's related.

To further enhance this security, HPE has added Aurora to its Greenlake Managed Services. Aurora extends the security of the "Worlds Most Secure Industry Standard Server" to all of the hosted applications and workloads, including VMs and containers. With this service enabled, the ability to detect malicious activity has been greatly enhanced and automatic recovery allows a hosted server, application or workload to be restored in minutes. In addition, this detection is not limited to boot: Applications are monitored while the server is running and any unwanted activity will allow the application to restored immediately.

The benefits are many. GreenLake uses a consumption-based model, which helps avoid heavy upfront costs and pricey over-provisioning; scaling is simple; and you maintain self-service agility for deploying resources, reviewing spend and forecasting capacity. Or you can choose to offload the effort with GreenLake management services, which handles the routine IT work: monitoring, operations, administration, optimization and nearly continuous improvement.

Don't Let Your District Be the Next Victim

School leaders need to be cognizant of the fact that their own district could easily be the next ransomware victim. It's time for them to open their eyes to the risks the district faces and start moving in increments to provide a safer online environment for the school community. There are plenty of sources for getting the help that's needed.

***James Morrison** is a distinguished technologist in cybersecurity for Hewlett Packard Enterprise. Prior to working with HPE, he served 22 years in the U.S. government, including a lengthy period with the Federal Bureau of Investigation working as a computer scientist, among other roles.*