Public school district experiences the headache of navigating ransomware and cryptocurrency.

What happened:
On April 14th 2018, the school district of Leominster, Massachusetts uncovered a ransomware infection that pervaded their network. Remediating the incident took over two weeks, including 6 days to make a payment.

According to school officials, a total of 25 systems were directly affected - 13 servers, 11 desktops and other connected devices, including the schools backup devices, were encrypted.

"Since back-up services were also affected, files which we might have been able to restore from were also encrypted, and in effect rendered them useless." *- Paula Deacon, Superintendent of Schools in Leominster*

Background context:
Small school districts often fall victim to ransomware campaigns. In Leominster's case, tight budgets lead to IT cuts the prior year. A number of devices were reportedly running older, possibly unpatched operating systems and a remote desktop protocol; two common access points for ransomware campaigns.

The school may have been accruing up to $21,000 per hour of downtime costs due to unproductive / idle labor.
- Coveware proprietary analysis

It is unlikely that Leominster was specifically targeted. They were likely caught in a dragnet ransomware campaign meant to snare exposed or unprotected endpoints. The acting Superintendent, Paula Deacon, remarked, "All it takes is for one person to open up one tab." We have on our end 900 staff and almost 6,300 students using PCs every single day. We had thousands of systems impacted."

Remediation options:
When ransomware hits organizations like Leominster two options are generally available: attempting to restore systems and recover lost data from backups or pay the ransom demand.

Restoring backups may be time consuming and costly. IT service hours are necessary to restore, configure and test each machine in need of recovery. However, Leominster reported that their back up systems were also encrypted, likely hampering their restore options.

The choice to pay ransom is often the final option, yet ransom payment comes with no guaranty that valid keys to unlock the encryption will be provided. It is estimated that over 80% of payments result in the keys being provided, so the decision is often justified by pure economics.

80% of of businesses that experience a ransomware infection and pay, would pay again. *-Telstra Security Report 2018*

Economic reality:
Frequently, the economic decision is clear when comparing the downtime costs to the cost of the payment. In the case of Leominster, downtime costs were upwards of $21,000 per hour. The $10,000 ransom was the equivalent of less than an hour of downtime.

"If we had not used the option of paying the ransom for the decryption of our files, we would most assuredly be in for a much longer recovery at a much higher cost." *- Paula Deacon, Superintendent of Schools in Leominster*

Ending downtime was clearly the priority. As downtime costs compounded, the Leominster school made the decision to pay and the superintendent was confident in their conclusion.

Crypto delays:

But then came an another unexpected hurdle: how to pay. "We had to come up with $10,000 in a legal way," Mayor (and School Committee member) Dean Mazzarella said. "You just can't, somebody calls us and says give us $10,000." Not only did the school district have to procure an approved expense, they also had to navigate the complexity of the cryptocurrency markets and wallets.

"It took six days for the school district to send cryptocurrency, "It's all being done through Bitcoin. It's very convoluted." *-Interim Leominster Police Chief Michael Goldman*

Six additional days of downtime due to cryptocurrency payment friction was an unanticipated delay for the school district, and one that other organizations will likely experience if they are not prepared.

"It is a lot of pressure to take on, especially as downtime mounts.

Coveware can help:

Using Coveware, an organization can lean on a fully automated SaaS solution for ransomware case analysis, and if necessary charge a ransom payment directly to a credit card to make a low latency cryptocurrency payment in minutes, rather than hours or days.

Coveware's solution shoulders a lot of that burden, dramatically improving the experience, and most importantly shrinking the time to recover."
-Adam Wipp, Helm MSP

As organizations and businesses assess their business continuity and disaster recovery investments, cases like Leominster demonstrate the importance of having more than one option available when ransomware strikes.

Contact us!
info@coveware.com
www.coveware.com

Disclaimer: All quotations for this case study are from from public news stories, public data sources, or Coveware proprietary analysis. No officials of Leominster town or school district provided input on this report.