MMUA

# Yes, it can happen to you: Thief River Falls shares its experience of cyber attack

Of all the threats municipal utilities have faced over the years, perhaps none is more insidious than a cyber-security intrusion.

And it can happen to you.

City of Thief River Falls staff were working after-hours in December 2020, installing a new billing system. While setting up a new firewall, staff received a notification that they couldn't log-in to the network, followed by a ransomware notification message.

In quick succession, staff was confronted with a back-up failed error, a red light on a firewall, erased firewall logs, and data being encrypted.

The first call city staff made went to a council member and IT professional. Initial steps to assess the situation were taken. The various city department heads were called in. It was determined that only certain computers were affected—those running malware protection software didn't appear to be affected.

A loaner server was obtained as a back-up on an interim basis and the city quickly hired Morris Electronics to help it through the troubles.

"They saved us," said City of Thief River Falls Electric Superintendent Dale Narlock. "They were on it right away."

City staff, with the extra help, proceeded to recover most of its data.

In the meantime, the city was receiving ominous messages. The first said that the criminal(s) had copied most of the city's data and that the city should "contact us." The would-be extortionists asked for $500,000, payable in crypto currency. After a week that request went to $1 million.

The city didn't respond.

Over the course of the next weeks it became increasingly clear that the city and its customers had escaped serious damage. Physical operations, including utility operations, were threatened but not affected. It was, however, a time of intense activity.

With the breach isolated, work was underway to remediate the city's computer network.


The City of Thief River Falls electric department serves several large, international corporations, including Arcto (Arctic Cat) and Digi-Key.

Among the thorny questions was, what to do with the billing system changeover: should work go forward or back?

It went ahead.

While the source of the breach was not definitely identified, there were several possibilities. It may have been a combination of a phishing email with social engineering, in the guise of offering help with a technical issue.

Many city employees were working from home at this time of COVID-19 response. New procedures were developed and firewalls installed.

The network architecture was changed, so that the ability to move from one computer to the next was made much more difficult.

In the end, the city lost its League of Minnesota Cities Insurance Trust (LMCIT) deductible of $25,000, racked up some staff overtime and unbudgeted consulting bills. It counted itself fortunate, however, and is much more wary of cyber-security issues going forward.

"Don't be too comfortable," Narlock said.

For more information, contact the LMCIT or your trusted IT professional.

## Federal cyber-attack reporting law adopted

On March 10, the U.S. Congress passed legislation that mandates critical infrastructure providers and federal agencies promptly report cyberattacks and ransomware payments to the Cybersecurity and Infrastructure Security Agency (CISA). The historic reporting requirements are part of a $1.5 trillion omnibus spending bill.

The law requires critical infrastructure organizations in 16 industry sectors identified by the federal government, including the energy sector, to report to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours if they are experiencing a cyberattack, and within 24 hours of making a ransomware payment.

The law further stipulates that CISA will have the authority to subpoena organizations within the identified industry sectors that fail to report cybersecurity incidents or ransomware payments and can refer non-compliant organizations to the Department of Justice.

Critical Infrastructure Protection (CIP) rules overseen by the North American Electric Reliability Corp. already require utilities to report some attacks.