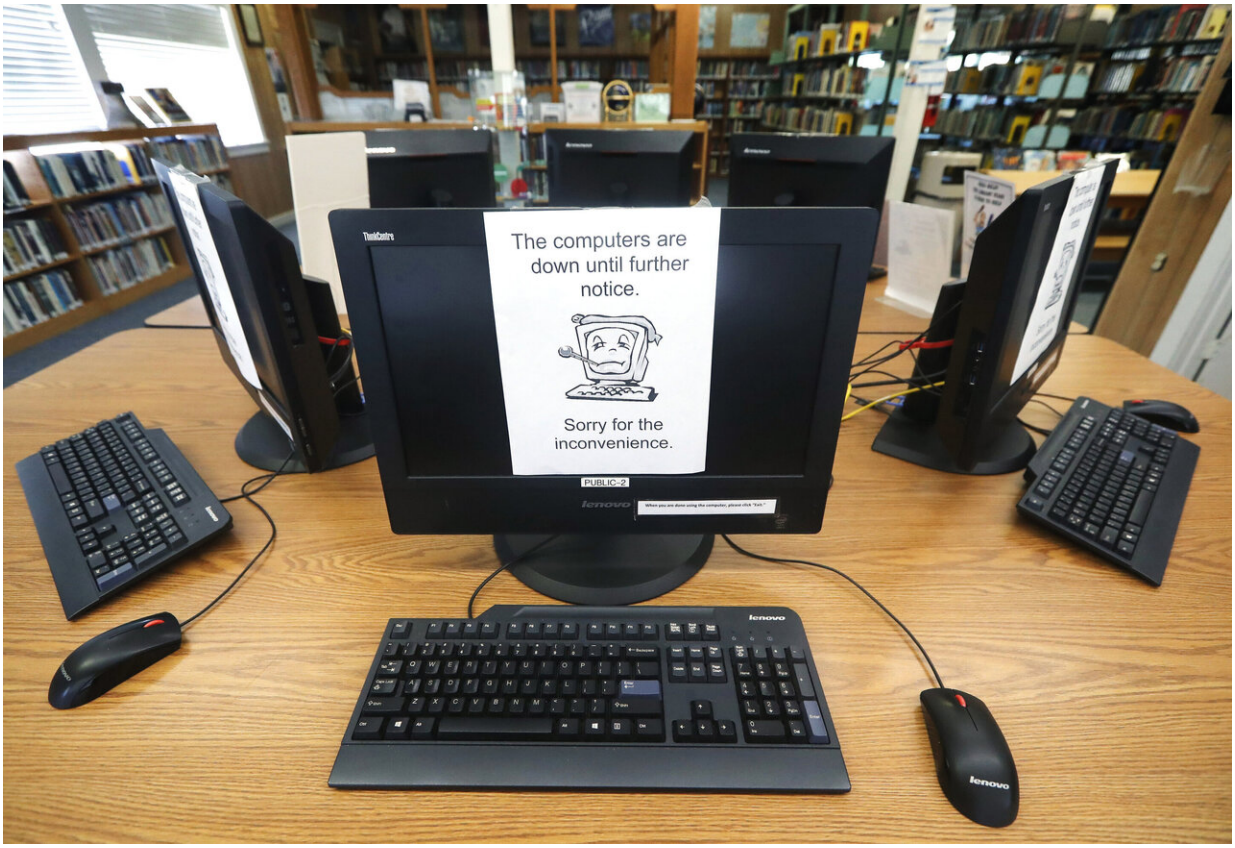
Payouts from insurance policies may fuel ransomware attacks

September 20 2019, by Kathleen Foody



In this Aug. 22, 2019, file photo, signs on a bank of computers tell visitors that the machines are not working at the public library in Wilmer, Texas. Some cybersecurity professionals are concerned that insurance policies designed to limit the damage of ransomware attacks might actually be encouraging hackers. Twenty-two local governments in Texas were hit in August. (AP Photo/Tony Gutierrez, File)

The call came on a Saturday in July delivering grim news: Many of the computer systems serving the government of LaPorte County, Indiana, had been taken hostage with ransomware. The hackers demanded $250,000.

No way, thought County Commission President Vidya Kora. But less than a week later, officials in the county southeast of Chicago agreed to pay a $132,000 ransom, partially covered by $100,000 from their insurance provider.

"It was basically an economic decision," Kora said. "How long do you keep all these employees sitting, doing nothing? Whereas if you pay this, we can be back up and running."

That's precisely the calculation hackers count on. Now some cybersecurity professionals are concerned that insurance policies designed to limit the damage of ransomware attacks might be encouraging hackers, who see insurers covering increasingly large ransoms and choose to target the type of institutions likely to have coverage.

"Once a cybercriminal finds a formula that works for them, they're going to stick to it," said Tyler Moore, a cyber security professor at the University of Tulsa. "If you're a company or a city that has this coverage, the decision of whether to pay is quite clear. It gets more difficult when you take a step back and look at the societal view."

This year alone, the average ransom payment climbed from $12,762 at the end of March to $36,295 by the end of June—a 184% jump—according to Coveware, a firm that negotiates on behalf of ransomware victims.

Officials have cited insurers' help paying ransoms in recent high-profile

hacks, including those in several Florida cities that paid six-figure ransoms. Elected officials reassured the public that taxpayers were only accountable for a deductible.

The mayor of New Bedford, Massachusetts, acknowledged this month that city officials offered to pay $400,000 after ransomware locked up 158 city computers in July. The hackers had demanded $5.3 million.

In a statement released two months later, Mayor Jon Mitchell said he was initially reluctant to negotiate, but he eventually concluded that it would be "irresponsible" to dismiss "the possibility of obtaining the decryption key if insurance coverage could cover the full cost of the ransom payment."

New Bedford never received a counteroffer from its hackers. Insurance coverage through AIG is expected to help with the cost of recovering lost files and upgrading security, Mitchell has said.

In this Sept. 12, 2019, photo, monitors check their screens in the Governor's Office of Information Technology in Denver. Some cybersecurity professionals are concerned that insurance policies designed to limit the damage of ransomware attacks might actually be encouraging hackers. "We don't know what that ransom payment is going to fund," said Brandi Simmons, a spokeswoman for the office. "As a state government, we don't want to be in a position of funding cyberterrorists." (AP Photo/David Zalubowski)

The earliest use of ransomware came in the late 1980s. Attackers often launch their assaults via email containing malicious links or attachments. Once they have access, they encrypt files, databases and entire computer networks until the ransom is paid.

In recent years, ransomware has become much more common, fueled by cryptocurrency that makes it easier for hackers to receive and then spend the payouts. Twenty-two local governments in Texas were hit in August . Businesses aiming to thwart hackers or repair their damage have grown rapidly in response, including insurance providers offering policies that cover ransom payments.

Insurers do not release detailed information about clients' experience with ransomware, so it's difficult to know how often victims agree to pay. One 2016 study by the nonprofit Cloud Security Alliance found that companies with insurance were more likely to pay a ransom to hackers threatening to release sensitive information— 28% compared with 22% for companies without insurance.

La Porte County officials purchased a cyber security policy in 2018, months before they got hit, Kora said. The insurance company, Travelers, sent a law firm and a cybersecurity team to try to restore the computer systems and simultaneously negotiate with the hackers. The county also reported the ransomware to the FBI.

No one was able to free the encrypted information, Kora said. For days, the county's criminal and civil courts stalled without access to records, databases and payment systems. Employees in other county offices had no access to email or electronic records.

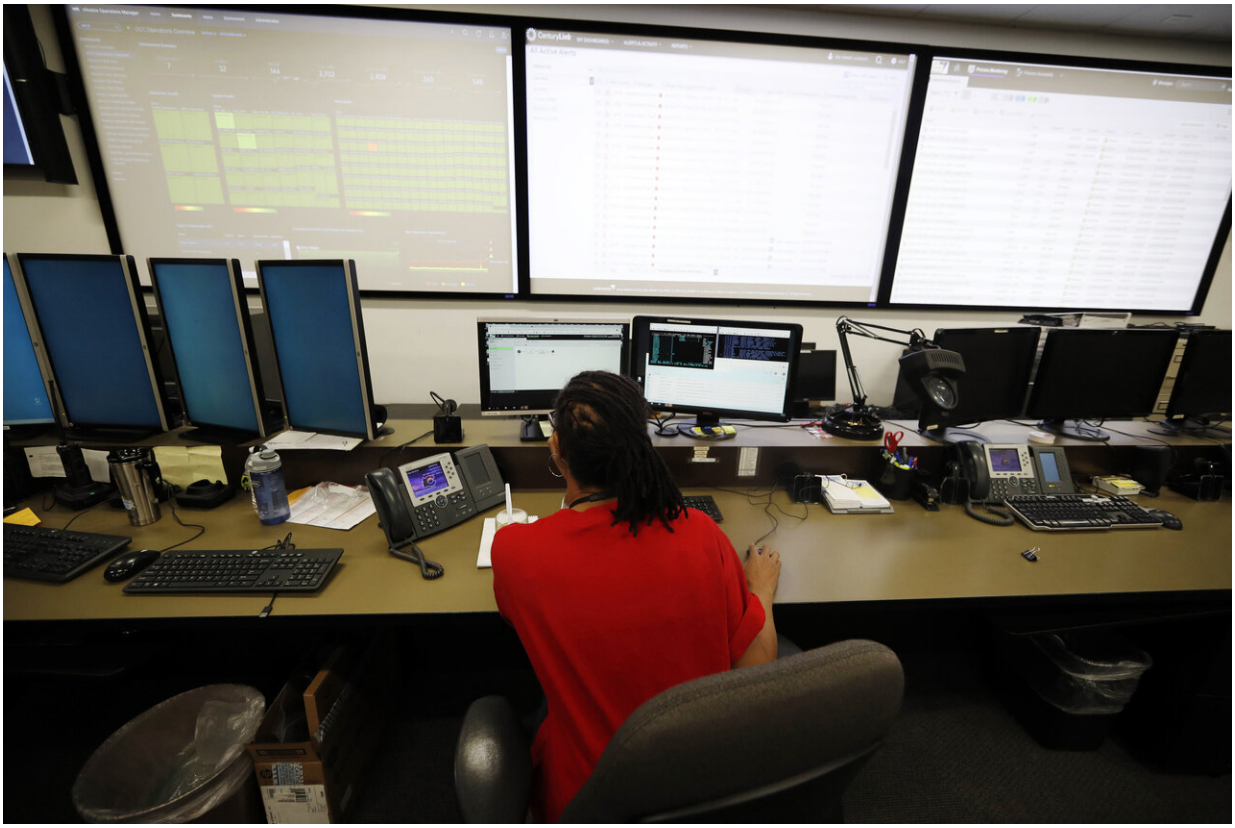
LaPorte County's policy covered up to $100,000 toward a ransom payment. Feeling trapped, county commissioners decided to cover the remaining $32,000.

Texas officials have released little information on the ransomware that hit local governments, including the hackers' specific demands. The Texas Department of Information Resources said in a statement released Sept. 5 that it was not aware of any community paying a ransom.

According to the FBI, more than 1,400 instances of ransomware were reported last year, and victims reported paying $3.6 million. But former officials said that's undoubtedly a fraction of the true picture because many victims don't report, fearing damage to shareholders and loss of customers' trust.

Government agencies often don't have the option to keep quiet.

Cindy Pfeifer, clerk and treasurer of the Wisconsin village of Nashotah, was facing deadlines for property tax collections, budget preparations and completion of employees' tax documents when she began a late November workday. But her computer was useless. It had been locked by hackers demanding $10,000.



In this Thursday, Sept. 12, 2019, photograph, monitors check their screens in the Governor's Office of Information Technology in downtown Denver. Some cybersecurity professionals are concerned that insurance policies designed to limit the damage of ransomware attacks might actually be encouraging hackers. "We don't know what that ransom payment is going to fund," said Brandi Simmons, a spokeswoman for the office. "As a state government, we don't want to be in a position of funding cyberterrorists." (AP Photo/David Zalubowski)

"My stomach still clenches when I think about it," Pfeifer said.

Technology staff for the village of 1,357 residents negotiated the hackers down to about $2,500. Officials paid, fearing that rebuilding records would cost much more.

Josephine Wolff, a professor of cybersecurity policy at Tufts University, fears that insurance coverage of ransom payouts gives victims distance from the ripple effect of their decision.

"By saying, 'Oh, this is just something my insurance covers,' they're forgetting that is contributing direct financial resources to future criminal operations," Wolff said.

That effect has kept some targets from making ransom payments. After hackers locked systems for vendor and employee payments at the Colorado Department of Transportation, state officials resolved not to give in. Restoring the systems cost up to $1.5 million.

"We don't know what that ransom payment is going to fund," said Brandi Simmons, a spokeswoman for the governor's office of technology. "As a state government, we don't want to be in a position of funding cyberterrorists."

Insurers said the decision about paying a ransom is ultimately the victim's and not dictated by the terms of a policy, but it does require consideration of practical questions, said Michael Tanenbaum, head of the Cyber North America division for Chubb insurance.

How long can they operate without access to the data? Do they have functioning backups to use while experts try to get the data back? What if the stolen data can't be recovered?

Executives of a multinational company that makes $10 million a day may not blink at paying $10,000 to get data back. A $10 million ransom, though, would take more thought, said Howard Marshall, a former deputy assistant director of the FBI's cyber division, who now leads the cyber threat intelligence team at the consulting firm Accenture.

"The time for that thought process is well in advance," he said, "not when the attacker's clock is ticking."