RANSOMWARE ENABLERS

The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks

Even when public agencies and companies hit by ransomware could recover their files on their own, insurers prefer to pay the ransom. Why? The attacks are good for business.

by Renee Dudley | Aug. 27, 5 a.m. EDT

When Lake City, Florida, was paralyzed by a ransomware attack, an underwriter at Lloyd's of London recommended paying the ransom rather than trying to recover backup files. The Lloyd's building in London is pictured. *(Jack Taylor/Getty Images)*

RANSOMWARE ENABLERS
U.S. Companies and Cyber-Extortion

ProPublica is a nonprofit newsroom that investigates abuses of power. Sign up for ProPublica's Big Story newsletter to receive stories like this one in your inbox as soon as they are published.

On June 24, the mayor and council of Lake City, Florida, gathered in an emergency session to decide how to resolve a ransomware attack that had locked the city's computer files for the preceding fortnight. Following the Pledge of Allegiance, Mayor Stephen Witt led an invocation. "Our heavenly father," Witt said, "we ask for your guidance today, that we do what's best for our city and our community."

Witt and the council members also sought guidance from City Manager Joseph Helfenberger. He recommended that the city allow its cyber insurer, Beazley, an underwriter at Lloyd's of London, to pay the ransom of 42 bitcoin, then worth about $460,000. Lake City, which was covered for ransomware under its cyber-insurance policy, would only be responsible for a $10,000 deductible. In exchange for the ransom, the hacker would provide a key to unlock the files.

"If this process works, it would save the city substantially in both time and money," Helfenberger told them.

Without asking questions or deliberating, the mayor and the council unanimously approved paying the ransom. The six-figure payment, one of several that U.S. cities have handed over to hackers in recent months to retrieve files, made national headlines.

Left unmentioned in Helfenberger's briefing was that the city's IT staff, together with an outside vendor, had been pursuing an alternative approach. Since the attack, they had been attempting to recover backup files that were deleted during the incident. On Beazley's recommendation, the city chose to pay the ransom because the cost of a prolonged recovery from backups would have exceeded its $1 million coverage limit, and because it wanted to resume normal services as quickly as possible.

"Our insurance company made [the decision] for us," city spokesman Michael Lee, a sergeant in the Lake City Police Department, said. "At the end of the day, it really boils down to a business decision on the insurance side of things: them looking at how much is it going to cost to fix it ourselves and how much is it going to cost to pay the ransom."

The mayor, Witt, said in an interview that he was aware of the efforts to recover backup files but preferred to have the insurer pay the ransom because it was less expensive for the city. "We pay a $10,000 deductible, and we get back to business, hopefully," he said. "Or we go, 'No, we're not going to do that,' then we spend money we don't have to just get back up and running. And so to me, it wasn't a pleasant decision, but it was the only decision."

Ransomware is proliferating across America, disabling computer systems of corporations, city governments, schools and police departments. This month, attackers seeking millions of dollars encrypted the files of 22 Texas municipalities. Overlooked in the ransomware spree is the role of an industry that is both fueling and benefiting from it: insurance. In recent years, cyber insurance sold by domestic and foreign companies has grown into an estimated $7 billion to $8 billion-a-year market in the U.S. alone, according to Fred Eslami, an associate director at AM Best, a credit rating agency that focuses on the insurance industry. While insurers do not release information about ransom payments, ProPublica has found that they often accommodate attackers' demands, even when alternatives such as saved backup files may be available.

The FBI and security researchers say paying ransoms contributes to the profitability and spread of cybercrime and in some cases may ultimately be funding terrorist regimes. But for insurers, it makes financial sense, industry insiders said. It holds down claim costs by avoiding expenses such as covering lost revenue from snarled services and ongoing fees for consultants aiding in data recovery. And, by rewarding hackers, it encourages more ransomware attacks, which in turn frighten more businesses and government agencies into buying policies.

"The onus isn't on the insurance company to stop the criminal, that's not their mission. Their objective is to help you get back to business. But it does beg the question, when you pay out to these criminals, what happens in the future?" said Loretta Worters, spokeswoman for the Insurance Information Institute, a nonprofit industry group based in New York. Attackers "see the deep pockets. You've got the insurance industry that's going to pay out, this is great."

A spokesperson for Lloyd's, which underwrites about one-third of the global cyber-insurance market, said that coverage is designed to mitigate losses and protect against future attacks, and that victims decide whether to pay ransoms. "Coverage is likely to include, in the event of an attack, access to experts who will help repair the damage caused by any cyberattack and ensure any weaknesses in a company's cyberprotection are eliminated," the spokesperson said. "A decision whether to pay a ransom will fall to the company or individual that has been attacked." Beazley declined comment.

Fabian Wosar, chief technology officer for anti-virus provider Emsisoft, said he recently consulted for one U.S. corporation that was attacked by ransomware. After it was determined that restoring files from backups would take weeks, the company's insurer pressured it to pay the ransom, he said. The insurer wanted to avoid having to reimburse the victim for revenues lost as a result of service interruptions during recovery of backup files, as its coverage required, Wosar said. The company agreed to have the insurer pay the approximately $100,000 ransom. But the decryptor obtained from the attacker in return didn't work properly and Wosar was called in to fix it, which he did. He declined to identify the client and the insurer, which also covered his services.

"Paying the ransom was a lot cheaper for the insurer," he said. "Cyber insurance is what's keeping ransomware alive today. It's a perverted relationship. They will pay anything, as long as it is cheaper than the loss of revenue they have to cover otherwise."

Worters, the industry spokeswoman, said ransom payments aren't the only example of insurers saving money by enriching criminals. For instance, the companies may pay fraudulent claims — for example, from a policyholder who sets a car on fire to collect auto insurance — when it's cheaper than pursuing criminal charges. "You don't want to perpetuate people committing fraud," she said. "But there are some times, quite honestly, when companies say: 'This fraud is not a ton of money. We are better off paying this.' ... It's much like the ransomware, where you're paying all these experts and lawyers, and it becomes this huge thing."

Insurers approve or recommend paying a ransom when doing so is likely to minimize costs by restoring operations quickly, regulators said. As in Lake City, recovering files from backups can be arduous and time-consuming, potentially leaving insurers on the hook for costs ranging from employee overtime to crisis management public relations efforts, they said.

"They're going to look at their overall claim and dollar exposure and try to minimize their losses," said Eric Nordman, a former director of the regulatory services division

of the National Association of Insurance Commissioners, or NAIC, the organization of state insurance regulators. "If it's more expeditious to pay the ransom and get the key to unlock it, then that's what they'll do."

Share Your Story

We're Reporting on Ransomware. Do You Know Something About an Attack?

Has your organization been hit by ransomware? Did you hire a data recovery firm? Do you know how an attack works from the inside? We'd like to hear from you.

As insurance companies have approved six- and seven-figure ransom payments over the past year, criminals' demands have climbed. The average ransom payment among clients of Coveware, a Connecticut firm that specializes in ransomware cases, is about $36,000, according to its quarterly report released in July, up sixfold from last October. Josh Zelonis, a principal analyst for the Massachusetts-based research company Forrester, said the increase in payments by cyber insurers has correlated with a resurgence in ransomware after it had started to fall out of favor in the criminal world about two years ago.

One cybersecurity company executive said his firm has been told by the FBI that hackers are specifically extorting American companies that they know have cyber insurance. After one small insurer highlighted the names of some of its cyber policyholders on its website, three of them were attacked by ransomware, Wosar said. Hackers could also identify insured targets from public filings; the Securities and Exchange Commission suggests that public companies consider reporting "insurance coverage relating to cybersecurity incidents."

Even when the attackers don't know that insurers are footing the bill, the repeated capitulations to their demands give them confidence to ask for ever-higher sums, said Thomas Hofmann, vice president of intelligence at Flashpoint, a cyber-risk intelligence firm that works with ransomware victims.

Ransom demands used to be "a lot less," said Worters, the industry spokeswoman. But if hackers think they can get more, "they're going to ask for more. So that's what's happening. ... That's certainly a concern."

In the past year, dozens of public entities in the U.S. have been paralyzed by ransomware. Many have paid the ransoms, either from their own funds or through insurance, but others have refused on the grounds that it's immoral to reward criminals. Rather than pay a $76,000 ransom in May, the city of Baltimore — which did not have cyber insurance — sacrificed more than $5.3 million to date in recovery expenses, a spokesman for the mayor said this month. Similarly, Atlanta, which did have a cyber policy, spurned a $51,000 ransom demand last year and has spent about $8.5 million responding to the attack and recovering files, a spokesman said this month. Spurred by those and other cities, the U.S. Conference of Mayors adopted a resolution this summer not to pay ransoms.

Still, many public agencies are delighted to have their insurers cover ransoms, especially when the ransomware has also encrypted backup files. Johannesburg-Lewiston Area Schools, a school district in Michigan, faced that predicament after being attacked in October. Beazley, the insurer handling the claim, helped the district conduct a cost-benefit analysis, which found that paying a ransom was preferable to rebuilding the systems from scratch, said Superintendent Kathleen Xenakis-Makowski.

"They sat down with our technology director and said, 'This is what's affected, and this is what it would take to re-create,'" said Xenakis-Makowski, who has since spoken at conferences for school officials about the importance of having cyber insurance. She said the district did not discuss the ransom decision publicly at the time in part to avoid a prolonged debate over the ethics of paying. "There's just certain things you have to do to make things work," she said.

Ransomware is one of the most common cybercrimes in the world. Although it is often cast as a foreign problem, because hacks tend to originate from countries such as Russia and Iran, ProPublica has found that American industries have fostered its proliferation. We reported in May on two ransomware data recovery firms that purported to use their own technology to disable ransomware but in reality often just paid the attackers. One of the firms, Proven Data, of Elmsford, New York, tells victims on its website that insurance is likely to cover the cost of ransomware recovery.

Lloyd's of London, the world's largest specialty insurance market, said it pioneered the first cyber liability policy in 1999. Today, it offers cyber coverage through 74 syndicates

— formed by one or more Lloyd's members such as Beazley joining together — that provide capital and accept and spread risk. Eighty percent of the cyber insurance written at Lloyd's is for entities based in the U.S. The Lloyd's market is famous for insuring complex, high-risk and unusual exposures, such as climate-change consequences, Arctic explorers and Bruce Springsteen's voice.

As ransomware attacks crippled businesses and law enforcement agencies, two U.S. data recovery firms claimed to offer an ethical way out. Instead, they typically paid the ransom and charged victims extra.

Many insurers were initially reluctant to cover cyber disasters, in part because of the lack of reliable actuarial data. When they protect customers against traditional risks such as fires, floods and auto accidents, they price policies based on authoritative information from national and industry sources. But, as Lloyd's noted in a 2017 report, "there are no equivalent sources for cyber-risk," and the data used to set premiums is collected from the internet. Such publicly available data is likely to underestimate the potential financial impact of ransomware for an insurer. According to a report by global consulting firm PwC, both insurers and victimized companies are reluctant to disclose breaches because of concerns over loss of competitive advantage or reputational damage.

Despite the uncertainty over pricing, dozens of carriers eventually followed Lloyd's in embracing cyber coverage. Other lines of insurance are expected to shrink in the coming decades, said Nordman, the former regulator. Self-driving cars, for example, are expected to lead to significantly fewer car accidents and a corresponding drop in premiums, according to estimates. Insurers are seeking new areas of opportunity, and "cyber is one of the small number of lines that is actually growing," Nordman said.

Driven partly by the spread of ransomware, the cyber insurance market has grown rapidly. Between 2015 and 2017, total U.S. cyber premiums written by insurers that reported to the NAIC doubled to an estimated $3.1 billion, according to the most recent data available.

Cyber policies have been more profitable for insurers than other lines of insurance. The loss ratio for U.S. cyber policies was about 35% in 2018, according to a report by Aon, a London-based professional services firm. In other words, for every dollar in premiums collected from policyholders, insurers paid out roughly 35 cents in claims. That compares to a loss ratio of about 62% across all property and casualty insurance, according to data compiled by the NAIC of insurers that report to them. Besides ransomware, cyber insurance frequently covers costs for claims related to data breaches, identity theft and electronic financial scams.

During the underwriting process, insurers typically inquire about a prospective policyholder's cyber security, such as the strength of its firewall or the viability of its backup files, Nordman said. If they believe the organization's defenses are inadequate, they might decline to write a policy or charge more for it, he said. North Dakota Insurance Commissioner Jon Godfread, chairman of the NAIC's innovation and technology task force, said some insurers suggest prospective policyholders hire outside firms to conduct "cyber audits" as a "risk mitigation tool" aimed to prevent attacks — and claims — by strengthening security.

"Ultimately, you're going to see that prevention of the ransomware attack is likely going to come from the insurance carrier side," Godfread said. "If they can prevent it, they don't have to pay out a claim, it's better for everybody."

Not all cyber insurance policies cover ransom payments. After a ransomware attack on Jackson County, Georgia, last March, the county billed insurance for credit monitoring services and an attorney but had to pay the ransom of about $400,000, County Manager Kevin Poe said. Other victims have struggled to get insurers to pay cyber-related claims. Food company Mondelez International and pharmaceutical company Merck sued insurers last year in state courts after the carriers refused to reimburse costs associated with damage from NotPetya malware. The insurers cited "hostile or warlike action" or "act of war" exclusions because the malware was linked to the Russian military. The cases are pending.

The proliferation of cyber insurers willing to accommodate ransom demands has fostered an industry of data recovery and incident response firms that insurers hire to investigate attacks and negotiate with and pay hackers. This year, two FBI officials who recently retired from the bureau opened an incident response firm in Connecticut. The firm, The Aggeris Group, says on its website that it offers "an expedient response by providing cyber extortion negotiation services and support recovery from a ransomware attack."

Ramarcus Baylor, a principal consultant for The Crypsis Group, a Virginia incident response firm, said he recently worked with two companies hit by ransomware. Although both clients had backup systems, insurers promised to cover the six-figure ransom payments rather than spend several days assessing whether the backups were working. Losing money every day the systems were down, the clients accepted the offer, he said.

Crypsis CEO Bret Padres said his company gets many of its clients from insurance referrals. There's "really good money in ransomware" for the cyberattacker, recovery experts and insurers, he said. Routine ransom payments have created a "vicious circle," he said. "It's a hard cycle to break because everyone involved profits: We do, the insurance carriers do, the attackers do."

Chris Loehr, executive vice president of Texas-based Solis Security, said there are "a lot of times" when backups are available but clients still pay ransoms. Everyone from the victim to the insurer wants the ransom paid and systems restored as fast as possible, Loehr said.

"They figure out that it's going to take a month to restore from the cloud, and so even though they have the data backed up," paying a ransom to obtain a decryption key is faster, he said.

"Let's get it negotiated very quickly, let's just get the keys, and get the customer decrypted to minimize business interruption loss," he continued. "It makes the client happy, it makes the attorneys happy, it makes the insurance happy."

If clients morally oppose ransom payments, Loehr said, he reminds them where their financial interests lie, and of the high stakes for their businesses and employees. "I'll ask, 'The situation you're in, how long can you go on like this?'" he said. "They'll say, 'Well, not for long.' Insurance is only going to cover you for up to X amount of dollars, which gets burned up fast."

"I know it sucks having to pay off assholes, but that's what you gotta do," he said. "And they're like, 'Yeah, OK, let's get it done.' You gotta kind of take charge and tell them, 'This is the way it's going to be or you're dead in the water.'"

Lloyd's-backed CFC, a specialist insurance provider based in London, uses Solis for some of its U.S. clients hit by ransomware. Graeme Newman, chief innovation officer at CFC, said "we work relentlessly" to help victims improve their backup security. "Our primary objective is always to get our clients back up and running as quickly as possible," he said. "We would never recommend that our clients pay ransoms. This would only ever be a very final course of action, and any decision to do so would be taken by our clients, not us as an insurance company."

As ransomware has burgeoned, the incident response division of Solis has "taken off like a rocket," Loehr said. Loehr's need for a reliable way to pay ransoms, which typically are transacted in digital currencies such as Bitcoin, spawned Sentinel Crypto, a Florida-based money services business managed by his friend, Wesley Spencer.

Sentinel's business is paying ransoms on behalf of clients whose insurers reimburse them, Loehr and Spencer said.

New York-based Flashpoint also pays ransoms for insurance companies. Hofmann, the vice president, said insurers typically give policyholders a toll-free number to dial as soon as they realize they've been hit. The number connects to a lawyer who provides a list of incident response firms and other contractors. Insurers tightly control expenses, approving or denying coverage for the recovery efforts advised by the vendors they suggest.

"Carriers are absolutely involved in the decision making," Hofmann said. On both sides of the attack, "insurance is going to transform this entire market," he said.

On June 10, Lake City government officials noticed they couldn't make calls or send emails. IT staff then discovered encrypted files on the city's servers and disconnected the infected servers from the internet. The city soon learned it was struck by Ryuk ransomware. Over the past year, unknown attackers using the Ryuk strain have besieged small municipalities and technology and logistics companies, demanding ransoms up to $5 million, according to the FBI.

Shortly after realizing it had been attacked, Lake City contacted the Florida League of Cities, which provides insurance for more than 550 public entities in the state. Beazley is the league's reinsurer for cyber coverage, and they share the risk. The league declined to comment.

Initially, the city had hoped to restore its systems without paying a ransom. IT staff was "plugging along" and had taken server drives to a local vendor who'd had "moderate success at getting the stuff off of it," Lee said. However, the process was slow and more challenging than anticipated, he said.

As the local technicians worked on the backups, Beazley requested a sample encrypted file and the ransom note so its approved vendor, Coveware, could open negotiations with the hackers, said Steve Roberts, Lake City's director of risk management. The initial ransom demand was 86 bitcoin, or about $700,000 at the time, Coveware CEO Bill Siegel said. "Beazley was not happy with it — it was way too high," Roberts said. "So [Coveware] started negotiations with the perps and got it down to the 42 bitcoin. Insurance stood by with the final negotiation amount, waiting for our decision."

Lee said Lake City may have been able to achieve a "majority recovery" of its files without paying the ransom, but it probably would have cost "three times as much money trying to get there." The city fired its IT director, Brian Hawkins, in the midst of the recovery efforts. Hawkins, who is suing the city, said in an interview posted online by his new employer that he was made "the scapegoat" for the city's unpreparedness. The "recovery process on the files was taking a long time" and "the lengthy process was a major factor in paying the ransom," he said in the interview.

On June 25, the day after the council meeting, the city said in a press release that while its backup recovery efforts "were initially successful, many systems were determined to be unrecoverable." Lake City fronted the ransom amount to Coveware, which converted the money to bitcoin, paid the attackers and received a fee for its services. The Florida League of Cities reimbursed the city, Roberts said.

Lee acknowledged that paying ransoms spurs more ransomware attacks. But as cyber insurance becomes ubiquitous, he said, he trusts the industry's judgment.

"The insurer is the one who is going to get hit with most of this if it continues," he said. "And if they're the ones deciding it's still better to pay out, knowing that means they're more likely to have to do it again — if they still find that it's the financially correct decision — it's kind of hard to argue with them because they know the cost-benefit of that. I have a hard time saying it's the right decision, but maybe it makes sense with a certain perspective."

ProPublica research reporter Doris Burke contributed to this story.