A negotiation strategy to help cities and organizations minimize losses when their data are held hostage

March 5 2019, by Rob Matheson

Gregory Falco. Credit: Ian MacLellan

In ransomware cyberattacks, hackers steal a victim's sensitive data and threaten to publish or block access to it unless a ransom is paid. Across the globe each year, millions of ransomware attacks are carried out on businesses, cities, and organizations, costing billions of dollars total in payments and damages. Many technologies can thwart such cyberattacks, but MIT Computer Science and Artificial Intelligence Laboratory (CSAIL) and Department of Urban Studies and Planning (DUSP) researchers believe there's more to solving the issue than deploying the latest software.

Based on business negotiation strategies, the researchers designed a "cyber negotiation" framework, published recently in the Journal of Cyber Policy, that details a step-by-step process for what to do before, during, and after an attack. Lead author and CSAIL and DUSP researcher Gregory Falco, who founded the critical-infrastructure cybersecurity startup NeuroMesh, spoke to MIT News about the plan. He was joined on the paper by co-authors Alicia Noriega SM '18, a DUSP alumna; and Lawrence Susskind, the Ford Professor of Environmental and Urban Planning and a researcher for the Internet Policy Research Initiative and the MIT Science Impact Collaborative.

Q: What are cities, especially, up against with ransomware attacks, and why not just invent better technologies to defend against these attacks?

A: If you think about critical infrastructure, like transportation systems or water service networks, these are often run by city or metro agencies that don't have tens of millions of dollars to pay experts or companies to deter or combat attacks. Given that cities have amassed all kinds of data on resident activity or infrastructure operations, hackers target these treasure troves of data to sell on the black market. They disrupt critical urban infrastructure on a regular basis in the United States. If someone hacks into a traffic lights and changes the signals that are supposed to be sent to an autonomous vehicle, or if someone hacks smart meters and interferes with our energy system, public health and safety will be at risk.

Cities do have personnel—usually an individual or small team—in charge of protecting critical infrastructure. But, they need a lot more help. Ransomware is one of the rare cases where they can have direct communication with a hacker and can possibly regain control of their data. They need to be ready to do this.

Most of my research has been about using hacker tools against hackers, and one of the most effective hacker tools is social engineering. To that end, we created "Defensive Social Engineering," a toolbox of social engineering strategies that employ negotiation capacities to alter the way ransomware attacks unfold. Encryption and other high-tech tools won't help once an attack has begun. We have devised a cyber negotiation framework that can help organizations reduce their cyber risks and bolster their cyber resilience.

Q: What methods did you use to design your cyber negotiation framework? What are some examples of strategies in the plan?

A: Larry [Susskind] is the co-founder of the interuniversity Program on Negotiation at Harvard Law School. We have applied the best negotiation practices to defending critical urban infrastructure from cyberattack. The pathology of most ransomware attacks matches up nicely with what happens in other kinds of negotiations: First, you size up your opponent, then you exchange messages, and ultimately you try to reach some kind of agreement. We focus on all three cyber negotiation stages: before, during, and after an attack.

To prepare before an attack it is necessary to raise awareness across the organization of how to handle an attack if one occurs. Public agencies need attack response plans. During an attack, agencies have to figure out the costs of complying or not complying with the demands of an attacker, and consult their legal team regarding their liabilities. Then, if the circumstances are right, they need to negotiate with the hacker, if possible. After an attack, it is important to review what happened, share information with appropriate authorities, document what was learned, and engage in damage control. Cyber negotiation does not necessarily require paying ransom. Instead, it focuses on being flexible and knowing how to manipulate the situation before, during, and after an attack. This approach to negotiation is a form of risk management.

To validate our framework, we interviewed a sample of infrastructure operators to understand what they'd do in the case of a hypothetical ransomware attack. We found that their existing process could integrate well with our cyber negotiation plan, such as making sure they have good response protocols up and ready, and having communication networks open across their internal organization to ensure people know what's going on. The reason our negotiation strategy is valuable is because these operators all handle different pieces of the cybersecurity puzzle, but not the full puzzle. It's essential to look at the whole problem.

While we found that no one wants to negotiate with an attacker, under certain circumstances negotiation is the right move, especially when agencies have no real-time backup systems in place. A classic case was last year in Atlanta, where hackers cut off digital services, including utility, parking, and court services. The city didn't pay the ransom of roughly $50,000, and now they have paid more than $15 million in fees trying to figure out what went wrong. That is not a great equation.

Q: In the paper, you retroactively apply your framework to two real ransomware attacks: when

hackers locked down England's National Health Service patient records in 2017, and a 2016 incident where hackers stole data on millions of users of Uber, which paid a ransom. What insights did you glean from these case studies?

A: For those, we asked, "What might have gone better if they prepared for and used our negotiation framework?" We conclude that there were a number of specific actions they could have taken that might well have limited the damage they faced. NHS, for instance, needed greater awareness among its employees about the dangers of cyberattack and more explicit communications about how to forestall such attacks and limit their spread. (For the ransomware to be successfully installed, an employee needed to click on an infected link.) In Uber's case, the company didn't engage authorities and never conducted damage control. That in part led to Uber losing its license to operate in London.

Cyberattacks are inevitable, and even if agencies are prepared, they are going to experience losses. So, dealing with attacks and learning from them is smarter than covering up the damage. A main insight from all of our work is not to get bogged down in installing expensive technical solutions when their defensive social engineering actions that can reduce the scope and costs of cyberattacks. It helps to be interdisciplinary and mix and match methods for dealing with cybersecurity problems like ransomware.

More information: Gregory Falco et al. Cyber negotiation: a cyber risk management approach to defend urban critical infrastructure from cyberattacks, *Journal of Cyber Policy* (2019). DOI: 10.1080/23738871.2019.1586969

This story is republished courtesy of MIT News (web.mit.edu/newsoffice/), a popular site that covers news about MIT research, innovation and teaching.

Provided by Massachusetts Institute of Technology

Citation: A negotiation strategy to help cities and organizations minimize losses when their data are held hostage (2019, March 5) retrieved 4 May 2024 from https://phys.org/news/2019-03-strategy-cities-minimize-losses-held.html