How do you prepare for the unexpected cyber attack?

Stuart Madnick

Working Paper CISL# 2020-11

January 2020

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

How do you prepare for the unexpected cyber attack?

Stuart Madnick

Last fall, in Northern California, the United States experienced its first ever deliberate large-scale and long-lasting blackout. Fueled by fears of increased devastating fires due to its century-old equipment, the region's utility company shut off power to more than 1.5 million people forcing many evacuations. The impact was devastating; Michael Wara, a climate and energy expert at Stanford University, estimated the cost to California as up to $2.5 billion. For cybersecurity experts like myself, the blackout was a signal of just how precarious our reliance on electricity is, and how much we have to fear in cyberattacks.

Think about what would happen if a cyberattack brought down the power grid in New York or even just a larger part of the country. As we saw in California, people could manage for a few hours -- maybe a few days -- but what would happen if the outage lasted for a week or more? If a larger population was targeted with a cyberattack on a utility, is an evacuation of millions of people feasible or desirable?

Questions we should all be asking include: If the power grid is breached making electric-start backup generators unusable, what do we do? What's the backup plan for the backup plan? What happens to our food supply? Our water supply? Our sewer systems? Our financial systems? Our economy? Answering these questions requires systems-level thinking about how everything is connected and consideration of the interdependencies. For example, hospitals might have backup generators. But, what about the supply line for refueling? If the refueling stations need electricity to operate pumps, what is the plan?

Planning for the Unexpected

We all understand that there are certain catastrophes that can reoccur – such as hurricanes or wildfires. But, how do you prepare for a catastrophe that has never occurred before? We do not do well at addressing things that we have never seen before.

Consider what happened in 2017 when an area of Wyoming was hit by a strong wind storm that knocked down many large power lines. It took about a week to restore power due to heavy snow and frozen ground. Initially, water and sewage treatment continued due to backup generators. But the pumps that moved sewage from low-lying areas to the treatment plants on higher ground were not designed to have generators, since they could hold several days of waste. After 3 days with no power, they started backing up. The water then had to be cut off to prevent backed up waste water from getting into homes and the town had to be evacuated. As the spokesperson for the town stated: "This will probably be the longest time that we have had to close … in our history." No one had anticipated such a scenario or sequence of events.

The Wyoming windstorm and the California fire threats provide cybersecurity researchers with real life tests of what to expect when we don't know what could happen; we haven't faced a large scale cyberattack. Based on conversations I have had with experts in the field, we are as unprepared for a major cyber attack as Wyoming was for the windstorm and California for the fire threat, regardless of whether you're talking about the regional or city level, or the private

sector. As Professor Lawrence Susskind, in MIT's Urban Systems department, described it to me, "[In a cyberattack today] Millions [of people]... could be left with no electricity, no water, no public transportation and no waste disposal for weeks (or even months)."

Weeks and months, as it happens, are good estimates for how long it could take to come back online after an attack on a utility. A cyberattack can disrupt a traditional computer system by manipulating the software or erasing data, but the physical computer is still intact and, with various degrees of effort, the software and data can be restored. But a cyber-physical system, such as a generator or similar computer-control equipment, can be destroyed – i.e., made to explode. Repairing or replacing such systems can take weeks or even months, especially if many are destroyed at the same time since spare systems and parts are usually scarce, and often custom manufactured.

Evaluating Our Risk

Some have asked me why such a major cyber attack of this nature hasn't already occurred. I believe there are three necessary conditions for one to happen: opportunity, capability, and motivation.

Opportunity: Often factories and energy companies consider themselves "air gapped," that is not directly connected to the internet and therefore management views them as safe[1]. There are plenty of ways to "jump" that gap to launch a cyberattack, as the Iranians learned when their uranium enrichment facility was attacked by Stuxnet.

Capability: Given that there may be ways to "get in," do the attackers have the capability to do damage. There is also plenty of capability out there. Although much attention has focused on the major state actors, such as China, Russia, North Korea, and Iran, the reality is that an attacker does not need billions of dollars of funds and thousands of people. As I sometimes say, "The good guys are getting better, but the bad guys are getting badder faster." The tools to accomplish attacks are increasingly available on the Dark Web at decreasing costs, including cyber weapons stolen from the NSA and CIA. For example, the Ukraine power grid attack used spear phishing, industrial control, and disk wiping techniques that were all readily available on the black market, many of them previously stolen from NSA.

Motivation: So far, motivation has been our major saving grace. What does the attacker gain by shutting down the power grid of another country? In the case of kinetic warfare (e.g., a missile attack), the possibility of retaliation acts as a strong deterrent. Satellites easily spot the origin of the missile and retaliation is likely to soon follow. But those checks and balances do not work as well for cyberwarfare where plausible deniability is so easy, or even misdirecting the blame to someone else. As recently reported, "Groups linked to Russia's intelligence agencies […] had recently been uncovered boring into the network of an elite Iranian hacking unit and attacking governments and private companies in the Middle East and Britain — hoping Tehran would be blamed for the havoc."

[1] In reality, due to the needs for remote operation and maintenance, being "air gapped" is increasingly rare, though upper management might not always be aware of that.

Relying on the lack of motivation and luck is not a safe way going forward.

How to better prepare

There are at least three problems with the way that we have addressed such issues in the past that need to change:

Driving forward by looking through the rear view mirror: This is an old cliché, but very appropriate. We usually focus our future actions in response to the last cyber attack. Although that helps to prevent future reoccurrences, which is good, it does little to address the cyber attack that we have never seen before. In some bizarre cases, the attackers actually took advantage of what they knew that their target had done to respond to their last cyber attack to make their next cyber attack even more effective. There needs to be visionary thinking: not just what *has happened*, but what *could happen*.

Get overwhelmed by addressing the causes rather than the impacts: In trying to think about, and prepare for new cyber attacks, we often start by thinking about how the cyber attack might originate. Instead, we should focus on what can we do to minimize the damage. Our Cybersafety analysis method starts with a focus on what are we trying to prevent, and then what controls or facilities can minimize the possibility of that outcome. For example, as part of a cybersafety analysis of a company's central utility system, our team determined that a relatively inexpensive relay[2] costing about $6,000 could safeguard against a cyber attack targeting the automatic voltage regulator (AVR) of a generator. This upgrade would prevent $11M worth of direct damage to the generator in addition to preventing subsequent outage damage of cost of repairs and lost revenue. Of course, if many such generators were targeted at the same time, the resulting widespread power outage would be substantial and long term.

Don't consider overlooked interdependencies and the unique properties of cyber-physical systems: Based on our past experiences, most people, especially engineers working with physical systems, assume independent failures. That is, there is of course some chance that generator #1, which is a mechanical device, will fail at some point, But it is unlikely that generator #2 will fail at the same time, and extremely unlikely that generators #1, #2, and #3 will fail at the same time, etc. Considering the physical properties, those assumptions are reasonable. But a cyber attack that destroys generator #1 can just as easily destroy all the others at the same time. Our emergency preparedness needs to not only take this into account, but plan for it.

What we Risk By Not Imagining the Unknown

To illustrate the risks we face by not planning, consider again the California blackouts of 2019; 248 hospitals were in regions that lost power. "I can't over emphasis the calamity that these events cause at the neighborhood level. Hundreds of health care facilities don't have back-up generators," said Jack Brouwer, an engineering professor and director of the National Fuel Cell Research Center at the University of California, Irvine. Referencing the deaths caused by

[2] Somewhat like a circuit breaker.

previous wildfires in California, he said, “If you’re out of power for an hour, that’s fine, but for a couple of days — those lives count as much as those that would be lost in a fire.”

We can and should be much better prepared. We need more innovative and systems-level thinking -- and a sense of urgency to mitigate the impact of a major cyber attack – before it happens!

Acknowledgement: This research was supported, in part, by funds from the members of the Cybersecurity at MIT Sloan (CAMS) consortium.

Author: STUART MADNICK is the John Norris Maguire (1960) Professor of Information Technologies in the MIT Sloan School of Management, Professor of Engineering Systems in the MIT School of Engineering, and Founding Director of Cybersecurity at MIT Sloan*: the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity*. He has been active in the cybersecurity field since co-authoring the book Computer Security in 1979. Email: smadnick@mit.edu