THE ACADEMY OF ELECTRICAL CONTRACTING

PAPER PRESENTED BY FELLOW
KENT BAKER ('92)

IT COULD HAPPEN TO ANYONE:
MALWARE, RANSOMWARE ATTACKS AND
PROTECTING YOUR COMPANY

JUNE 2022

Academy of Electrical Contracting * 1201 Pennsylvania Avenue, NW * Suite 1200 * Washington, DC 20004
202-991-6259 * dsj@necanet.org

News of technology-related security failures have become a normal part of daily reporting in recent years and no wonder: On average, more than 4,000 ransomware attacks alone happen daily, a 300% increase since 2015. Targets of these attacks include home users, businesses, and government entities. In September 2019, Baker Electric was the target of one such attack.

The initial goal of this attack was to secure passwords and other data that would allow the malicious parties to siphon off funds from our bank accounts. When that failed, the strategy shifted to one of ransoming our data and systems by locking us out of our own networks.

My goal in this paper is to give you an insider's look at preparing for, responding to, and recovering from a malware attack. While none of us can ensure a complete lack of adverse impact of such an attack, we can prepare our companies – including our response plans – such that the damage is minimal and our core business can resume in as little time as possible.

The malware attack we experienced took place over the course of several weeks from first discovery to returning to full operation. Our first indication of a problem at hand came on September 17, 2019, when our IT team noticed a new icon in the corner of the window of our platforms. As they looked into it, our systems began failing. Within a half-hour, our networks started shutting down; our whole system was completely dark within 90 minutes. We couldn't even call out on landlines.

With our network systems and financial accounts locked down, critical business processes were affected including:

- Office and field payroll were blocked, which threatened the previously made timeline agreements with Unions.
- Accounts Payable and Receivable daily operations were inoperable for several days.
- Pre-Construction and Estimating missed bid deadlines.
- Construction was unable to efficiently manage field operations and purchasing.
- Satellite offices were also infected via the network.

This was not only a significant disruption to our overall company functioning but also to our employees as individuals as they lost productivity and, for some, faced delayed paychecks and/or were asked to utilize personal time off. The hit to moral was a consequence on top of the rest of the troubling effects.

Despite the daunting challenge of this situation, a number of proactive arrangements worked in our favor once we realized that the malware attack was in progress including:

We had already implemented financial and technological safeguards. These prevented the first goal of the attack – accessing our financial accounts directly – from being successful.

We already had cyber insurance. Our provider was one of our first calls once we realized what was happening. This insurance is offered by most major insurance companies and protects against damages resulting from exactly these kinds of threats, offsetting the losses and cost of recovery from a cyber attack.

Our provider was able to help us get the correct consultants in place immediately, potentially including:

- Forensic consultants who could determine what took place, the effect it had, and the best next steps to take.
- Resumption consultants who specialize in network recovery and rebuilding.
- Negotiators. You might imagine a crime drama as soon as you read that word and the function is the same; the job of negotiators during a malware attack is to negotiate the terms of ransom. In our case,

the perpetrators were slow to identify themselves and make demands and the negotiators were able to draw them out and get the discussion started.

- Privacy consultants who understand the ins and outs of the legal implications of a data incident.

We had already established a partnership with a professional network security company. Prior to the attack, the company had audited and fortified our network. Unfortunately, even the most advanced network security company can only safeguard against the known threats and the creativity of malware perpetrators is seemingly endless. That the partnership was already in place, though, meant a much quicker response once we reported the attack; they were our second call.

It was due to each of these resources that none of our data was compromised during this attack. While we experienced a number of other costs – loss of efficiency, damage to our reputation, and the significant expenses of recovery – had those resources not been in place, this would have been a far more damaging, potentially company-threatening, event.

In the moment, however, a tool much more basic and long-standing was our key asset: Communication.

First, we reached out to employees to explain to them that we were experiencing a "network incident." The language matters, both for clarity (for example, since our data was never stolen, we didn't experience what the professionals consider a "data breach") and to avoid undue panic.

We wanted to proactively make sure that our team knew details including:

- How this network incident would affect their work on a day-to-day basis.
- When/if they should come into work.
- How it would affect their payroll.

Moreover, it was important that our employees knew what to say, and what *not* to say, to external parties. It was important that vendors, unions, governmental contracts, and other partners received a clear and concise report of what was happening, what they could expect from us, and what we were doing to resolve the attack and get back to business as usual.

It was also important that no one in our organization used terms like "breached" or "hacked" as these terms have specific legal definitions and were not appropriate for the malware attack, we experienced.

This thoughtful communication was also a matter of honoring and maintaining a number of critical contracts. For example:

- Government contracts include a clause that they will be notified promptly in the event of a cyber attack.
- With our bookkeeping systems and financial accounts locked down, we were unable to meet the agreed-upon timetables of paying unionized workers, requiring new, short-term agreements on pay timelines until the incident was resolved.
- While purchasing was on hold, we also needed to contact our vendors to discuss new timelines and ensure flexibility in receiving needed materials on our new, imposed timeline.

Direct communication done quickly and thoughtfully helped us return to normal operations once we had regained full control of our network.

The process of recovering from a malware attack is expensive and labor intensive.

In addition to the expense of the various contractors brought in, the cost of which was offset by our cyber insurance, we also were forced to divert significant human, and

therefore financial, resources for many weeks to recover and return to normal operations.

The decision about whether the company can absorb the cost of refusing to pay the ransom and, instead, return to operation through other means is the foundational decision in such attacks. It's the decision that then determines the steps to come and the resources needed to accomplish those steps.

We'll never know who it was that attacked our systems; it turns out that cyber crime is such a well-established "industry" that there are professional negotiators to represent the perpetrators as well. While our IT team worked to restore our data from backups and other sources (such as email, the cloud, etc.), our insurance company was negotiating the terms of unlocking our system. The terms reached? A demand of $600,000.

Thanks to their dedicated efforts, our IT team was able to disinfect the hardware, re-install the software, and restore the critical data for operations themselves, saving us from having to give in to the random demand.

The forensic team determined that no data had been compromised. While we could not undo the harm that had been done, our proactive measures did prevent an expensive and challenging cyber attack from become far more damaging than it could have been.

My hope is that the lessons we've learned will help you avoid a malware attack or, in the event that your firewalls are also compromised, recover as quickly and easily as possible.

Our takeaways have included proactive steps including:

- Backup data **daily**, ensuring that the saved data is isolated from your network. Testing the integrity of the backups and the restoration process is also wise. In the midst of a crisis is not the time to discover that backups have failed or that the intended procedure has major holes.
- Purchase cyber insurance. You'll need more coverage than you think.
- Create an emergency response plan. You likely already have them for natural disasters; having one for malware attacks serves a similar purpose of providing a proactive blueprint for how to respond in the midst of crisis.
- Enable strong SPAM filters to prevent as many phishing emails as possible. These emails pose as requests from known institutions and sometimes even other members of the team and are formatted to look like the real thing. They can (and do) easily fool people into compromising security with just one click or download.
- Configure firewalls to block access to malicious or questionable internet addresses.
- Use cloud-based software and storage to ensure that data is available outside of your network; in essence, these services extend the value of your backups.
- Implement a strong password policy and use Multi-Factor Authentication on all logins. While these can be cumbersome, they add a valuable level of security to logins, making password-cracking malicious software ineffective.
- Establish a relationship with attorneys experienced in cyber crime. They can help you understand your contractual obligations to your customers in the event of a Data Incident and a Data Breach so you can respond quickly and effectively and avoid adding potential contract violations to an already challenging situation.

Perhaps most importantly, educate your employees. They are both your biggest asset in recovery and, unfortunately, your greatest threat as so many cyber attacks come in the form of phishing emails that require a discerning eye to avoid. Consider conducting regular training for your employees to bring

them up to date on recent scams and keep their sense of caution heightened.

If your network does come under attack:

- Isolate the infected computer(s) immediately by disconnecting them from the network fully, wired and wireless connections.
- Contact your cyber insurance company.
- Implement your security crisis management plan.
- Communicate with your employees. Communicate early and consistently.
- Tap into professional support in fighting the attack; do not try to do it on your own.
- Default to cellular plan data for text, communications, and interconnect connectivity in the likely event that your wired and wireless network is shut down.

There is not perfect protection for cyber attacks, and there are no seamless solutions. We ultimately spent a significant amount of money recovering, including hours to our IT department who worked around the clock restoring our network, and our payroll department working under the burden of getting over a thousand employees paid in a timely manner.

Still, by utilizing our suggestions for proactive preparation, including a plan that outlines the steps to take in the event of a malware attack, you can rebound, getting your company back online and your people back to work.

About Kent Baker

Kent Baker represents the third of four generations of Bakers to own and operate Baker Electric in Southern California. Started by his grandfather, Leroy Baker, in 1938, the company has expanded its geography and grown its ranks to roughly 1,000 employees strong over the years. Kent took the reins as president in 1982 after serving in the Army; at Baker Electric, he has served as Chairman since his son, Ted, stepped into the role of President. For all his professional accomplishments, though, what Kent most treasures is his family. “Our family is a very close family, and the greatest thing we have amongst ourselves is a lot of trust. That’s the whole thing.”

NOTES

Academy of Electrical Contracting * 1201 Pennsylvania Avenue, NW * Suite 1200 * Washington, DC 20004
202-991-6259 * dsj@necanet.org