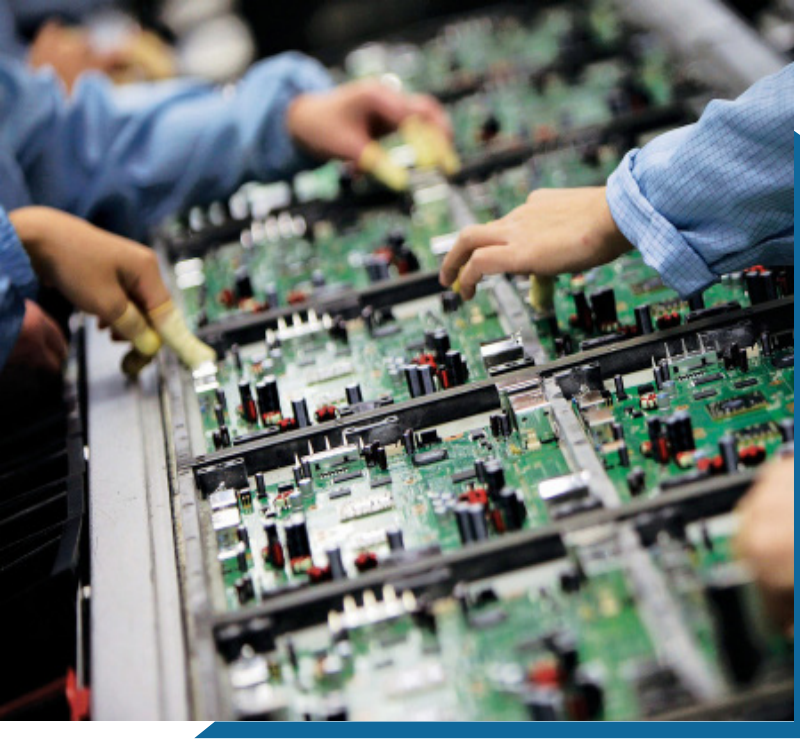

IGI

Solve. Simplify. Secure.

CASE STUDY

Manufacturing Industry

IGI worked with our partner, Dicar Networks, to help a large electronics company recover from multiple ransomware incidents and bolster its security posture to prevent future attacks. Read more about how IGI's incident response team helped them fully recover and put in the policies, processes, and technologies to protect from future attacks.

The Challenge

An electronic parts supplier—referred to as Customer in order to maintain their privacy—was working through a transition to a new, more secure network and firewall when they were faced with a cyber incident. During the transition when the Customer was the most vulnerable, their mission-critical infrastructure was attacked and the business was completely shut down.

"The sheer magnitude of having to recover that many systems at one time was overwhelming," the Customer said. "It took us a total of two months to get us back to 100 percent."

While dealing with the incident, the Customer's IT team simultaneously had to do recon to determine how this incident occurred. They found out there was an open port to a legacy terminal server that they didn't even know existed, which allowed the attackers to steal credentials and run a malicious script. You may hear about machines being attacked that are simply "sitting in a corner somewhere" and think it won't happen to your company, but that is exactly how this company became a victim of multiple ransomware attacks.

The first attack lasted 16 hours and the Company was shut down and cut off from customer contact for several days. The Customer then recovered one system at a time over two months to finally get back to its original state. But these attacks came with a one-two punch. Not long after recovering, another critical machine was hit with a Brute Force Attack, likely caused by residual damage from the original attack.

The Solution

Once the second attack hit, the Customer quickly worked with their MSP Dicar Networks to bring in a team of cybersecurity experts from IGI. Within 36 hours, IGI had identified the Customer's vulnerable areas and pinpointed key systems that were problematic.

"Had we known how vulnerable we were, we would have called IGI to deal with the original attack on that day," the Customer said. "I know that IGI would have prevented the second attack."

IGI immediately went through its full Incident Response process with multiple phases and implemented a Basic Threat Protection Package. During the Incident Response process, IGI not only found the two incidents that the Customer was aware of, but also uncovered malware from 2012.

IGI implemented additional solutions to further improve the Customer's security posture, including IGI's proprietary vulnerability management solution Nodeware™.

DICAR NETWORKS

The Result

This ransomware attack cost the Customer upwards of $2 million from downtime alone, which spanned over three days—1 day of attack and 2 days of recovery to get back up. If you look at time and personnel, the Customer estimates it was probably double that amount. The Customer said the ransomware delivered such a blow; they are still feeling the effects today. If they had implemented the solutions they have now, the cost would have been a fraction of that—if the attack ever occurred at all.

The biggest long-term obstacle for the Customer is what they described as "a big black eye" in the industry. Because they have some military and top-secret clients, their customers had major concerns over data being stolen. Fortunately, the Customer was able to work with Dicar Networks and IGI to produce a report that proves the data was uncompromised and putting customer concerns to bed. But there was certainly an impact to their reputation that they are working to mend.

The Customer calls the whole incident "an eye opener," that propelled them to work with IGI to put policies and procedures in place that would prevent future incidents. Now, the Customer has a solid Incident Response plan, an airtight reporting process, complete visibility of their network and vulnerabilities, and most importantly—peace of mind.

"IGI did a phenomenal job. It was good to have an expert set of hands—in addition to our IT experts internally. It made a big difference to work with people who do this every day," the Customer said. "I can see how smaller companies who don't have a full-time security person, or have someone without experience, that they may not ever recover from this."

The Customer also said they got "lucky" that their backup procedure was firmly in place before the attacks, so they were able to recover to about 99%. The biggest lesson, according to the Customer, was to act immediately and bring in the experts. They learned in just a few days how devastating ransomware can be, and how working with an experienced team can mean the difference between a full recovery with a newly secure network or the end of their business as they know it.

The Customer knows that security isn't a one-and-done task, it's an evolving process, which is the why the Customer is continuing to work with Dicar Networks and IGI on a recurring basis to keep their security posture at the level required to keep their business running smoothly.

> "IGI DID A PHENOMENAL JOB... IT MADE A BIG DIFFERENCE TO WORK WITH PEOPLE WHO DO THIS EVERY DAY"

FOR MATTERS OF SECURITY, THE IDENTITIES IN THIS CASE STUDY HAVE BEEN REMOVED AND DETAILS HAVE BEEN MODIFIED TO PROTECT CONFIDENTIALITY.

175 Sully's Trail, Suite 202
Pittsford, NY 14534

585.385.0610
855.385.0610

www.nodeware.com
www.igius.com