An Ideal Cyber Security Scenario

Rochester, NY — Since 2004, Ideal Manufacturing has delivered design support to building design and construction engineers. The company produces deep foundation products by highly skilled welders in a 60,000 square foot, ISO–9001 certified factory. Ideal's business has grown tremendously — in part due an enduring commitment to excellence in every aspect of their operations — including their computer infrastructure.

The company recently avoided what could have been a devastating amount of downtime to their manufacturing operations due to a zero-day exploit. They were quick to attribute it to heeding advice provided by SkyPort IT.

A zero day exploit is a cyber attack that occurs on the same day a weakness is discovered in software, which usually takes place before a software fix or patch has been released from the application developer. Because Ideal's IT network is secured with products that are layered on different levels of what is called a "vector' or point of potential intrusion, SkyPort IT was able to

detect the attempted cyberattack, thereby circumventing any potential ransomware demand.

To protect Ideal's network, SkyPort IT has spent three years improving their IT infrastructure at two of their NY locations. During this time, Ideal invested money into their IT infrastructure and incorporated many of the suggestions that SkyPort IT made regarding new technology, products and services that would help to detect and prevent hackers and ransomware attacks.

"We help companies safeguard their data by providing cyber security solutions. We also manage all levels and layers of their IT infrastructure," said Dan Marcellus, president and chief executive officer, SkyPort IT.

"Our IT system withstood a zero-day attack with less than half hour of down time and no data loss," said Dave Frink, manager, Ideal Manufacturing. Dave says the investment that Ideal has made in technology and services saves them money every day.

"I can't even imagine how much money we saved on the day of the attack," added Dave. "I have heard of companies

> *that have been put out of business by ransomware. But for us it was hardly a blip on our radar."*

One of the layers of protection that helped when hackers entered the Ideal network was the backup system. "The depth of the back up system was strong enough that it allowed us to recover any files that were affected by the intrusion," said Dan. "One of the main levels of protection is to ensure that proper permissions are set on the server so that the files that could be accessed by ransomware were minimized."

"Dan gives me realistic, step-by-step suggestions built around careful listening to our present needs, our projected needs and our resources, and takes extra steps to not over-sell equipment or services," said Dave.

SkyPort IT provides monthly reports to its managed data security services' clients as part of regular strategy meetings. The monthly report gives executive management an overall summary of the health of their entire computer network. Included is a one page overview of that month's activities including anti-virus compliance, computer patches, and a report description for each layer of SkyPort It's protective service.

Dan adds that in every IT protection scenario, the most important factor is preventing human error, which often is caused by lack of cybersecurity awareness and training. To head off mistakes, SkyPort IT provides employee awareness training, testing, policies and procedures, in addition to managing security services.

"We can put all these layers of protection in but a trained end user is still our last defense," he noted.