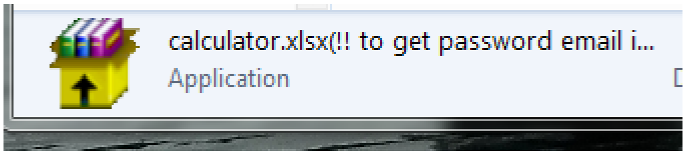
Losing It All- Why Cyber Security Must Be Addressed



calculator.xlsx(!! to get password email i...

Application

Ryan Cropper, owner of Able Body Shop, with three locations in Anchorage, Alaska, nearly lost everything on his personal office computer. By chance, he had come into his office on a Saturday morning to catch up on some work. He turned on his computer and all the icons he was used to seeing were now what looked like little gift boxes with books in them. It was a gift alright, a really bad one. When he clicked on one it had instructions on what he needed to do if he ever wanted to use his computer or see his files again. Ryan's computer had been attacked… and access to it, and all his data associated with it, were now being held for a $4,000 ransom. No negotiation. Take it or leave it. What a nightmare!

Ryan immediately contacted his IT guy who logged into Ryan's system remotely and saw what had happened. He did some research and found out that this professional hacker was from somewhere in Russia. This hacker makes pretty good money doing it. He demanded $4,000, not by traceable check or credit card, but by BitCoin, cyber currency that can be sent without the ability to track where it is really going. This hacker was scanning local companies looking for any open ports he could hack into, and, in Ryan's case, it was an open port he uses to gain remote access to his computer when he travels. That's all it took and this guy hijacked Ryan's system and held it for ransom. Now what to do…

Ryan weighed what it would take to simply shut everything down and start over. He considered the hours and hours it would take to recreate everything. Thankfully, none of the data was employee or customer personal data. Ryan had backups of his data (which we should all have), but starting over with software installation and setup, email system setup, etc., was just too big and expensive to contemplate. So, $4,000 seemed like the *"easier"* way out, albeit financially painful. He paid the ransom, not really knowing if he would ever get things back together or not. There was no way to know for sure. He waited. And waited. Finally, three days later, he received an email with a password that would get him back into his system. It worked, and he was back to business as usual. Well, not really *"as usual"*…

Nope, if you are a victim of a cyber-attack like this you never conduct business *"as usual"* again. It changes you. In Ryan's case he was fortunate enough to have insurance, including cyber liability/social engineering coverage, which covered his loss, minus a $500 deductible. Then he beefed up his online security and set up multiple layers of highly encrypted passwords.

How do you protect yourself? You don't really need to be an expert in any of this, you just need to know the steps to take to help block these attacks as best you can. Firewalls, closing open ports (with IT staff support), Norton or other top shelf software and employee policies, with enforcement, all help. David Willett, the automotive industry General Manager at Intrepid Direct Insurance, assisted me in researching this topic and shared that Intrepid has an insurance plan available that includes a special browsing tool, a sample Security Awareness and Training Policy for staff, and online staff training to help educate and defend against malicious ransomware attacks. You really need a network and data security policy in place, and regularly updated, for your employees. A sample copy can also be found on my website, www.optimaautomotive.com/cyber_security.

Because there is too much to get into here in a 750-word column, I have created a 1-hour long workshop on Cyber Security that is approved for AMI credit. It will cover examples like what Ryan experienced, steps you can take to protect yourself and includes information on the kind of insurance you should have to cover any loses you might suffer. You can access this online workshop at www.optimaautomotive.com/workshops.

There are many steps you can take to make it harder for hackers to hit you, but nothing is impenetrable. Hackers usually don't waste much time when they hit walls. They just move on until they can find an easy way in somewhere else. But, just in case, you should have some insurance in place to protect you financially. Take this workshop I'm offering, get insurance and build your defenses. You don't want to lose it all. Just ask Ryan.