**Have You Included Cybersecurity In Your CapEx Plans?**

A recent article appearing in the July/August issue of Chief Executive magazine, “Cybersecurity:The Battle Continues”, written by Peter Haapaniemi sparked the question that led me to think about how many of Idealliance’s members are incorporating some consideration of cybersecurity in their business planning processes. More specifically, I’m curious about how many of you are actually planning to spend money to protect important company data.

Some of you may be thinking that cyberattacks only happen to publicly traded, Fortune 500 companies. We’ve all read about the major cyberattacks on major companies and retailers. Even entire nations are being attacked as sophisticated crimeware, developed by rogue nations, is being given to organized crime groups for the purpose of extortion. However, I would suggest that the time is near when any dissatisfied customer, or angry ex-employee can access easy to obtain crimeware to launch an attack on any of our companies or organizations. Or, a contract or business relationship with a much larger company may expose you to risk. And, with many of us moving our data management to cloud based solutions we may be more vulnerable than ever.

*What Can You Do?*

* Begin by educating yourself and your team. Learn from experts in the field of cybersecurity. For example, the article mentioned above makes the following points –
	+ Your IT department is still the key to security. They need to make sure you are consistent with all best practices related to IT security.
	+ Become familiar with current corporate security technologies. Make sure that any technology you employ does not violate legal or ethical boundaries.
	+ Understand the risks associated with entrusting a cloud provider with your data. While there are obvious risks you should be familiar with, you should also know that most reputable cloud providers employ more sophisticated approaches to security than most small or mid-sized companies.
	+ Understand that the weakest point in your approach to cybersecurity is not related to the systems or technology you use, but more dependent on the people you employ. One motivated employee can render even the most sophisticated defense system useless. The article points out that you need to consider vendors, supply chain partners, and ex-employees as well.
	+ CEO’s and other executives who have easy access to important systems and data represent a risk as well. The article points out that the “FBI reported last year that spear-phishing scams that use fake executive e-mails to direct payments to phony vendors had cost companies $2.3 billion in the previous three years.”
	+ You may want to consider developing a contingency plan that would lay out your response to an attack.
	+ Most of us can’t afford to hire a Chief Information Security Officer, but someone on staff should be given the responsibility of becoming your company’s cybersecurity expert. Again, being informed and educated is the most important first step you can take to protecting your company from an attack.

Returning to the first question, I’m most interested in what, if anything, you are doing related to the threat posed by cybercriminals.

I would welcome transferring this dialog to our Open Forum where various positions and questions can be explored by our entire membership.

Thank you for your consideration.