Considerations and thoughts on

**Cyber Crime Issues**

From the Insurance Center Group, Inc.

* Attacks on small(er) businesses are growing at a rapid pace, as they are susceptible to cyber-crime for the same reason most criminals target their victims - it is easy. It is probably not if, but when, it will happen and if it is successful!
* **Data Breach** crimes are not limited to your computer files. Lost paper files, employees selling information (or being vengeful), or unknown disappearances can happen as easily as a lost laptop or an internet hacker break in.
* Cyber-crimes are not limited to loss of data. **Ransomware** (extortion by taking control of your computer and requiring money to unlock it; or lose your information and/or not being able to do business) is on the rise, due to the ease of monetizing (crypto currency) and availability of “ransomware for rent”.
* **Cyber Deception** (Social Engineering) is also increasing. Tricking employees into divulging information, allowing access to bank accounts, is on the uptick due to the sophistication of today’s technology.

How is it happening?

* Most losses are caused by malicious attack, human error, and computer system issues/weaknesses.
* Most frequent insurance claims are ransomware extortion, social engineering, and general business interruption.
* Majority of losses are due to errors by people, not by brute force entry. Mostly by -
1. Opening “bad intention” (phishing/spoofing) emails or attachments
2. Unauthorized or unintentional (spoofing) website visits
3. Weak, or not updated, or repeatedly used passwords
4. Deception leading to unauthorized funds transfers

How might it impact you?

* Can your business function without your computers for days? Weeks?
* Can you survive if your business is shut down; or impacted by loss of reputation?
* Can you pay for the required or demanded remedies and other costs?

Are you at risk?

* Yes, if you have employees (or you yourself) who are not, or don’t have time to be, an informed and competent cyber expert. And even if you take steps to avoid the issue.
* Average loss per category (remember it takes some much larger losses to make an average!) -
1. Data Breach - $180 per “lost record” (example - $180 x 5000 = $900,000). Normal range is between 2,000 and 101,000 records lost.
2. Ransomware - $200,000 average\*. 40% increase in frequency.
3. Cyber Deception - Around $100,000.

What can you do?

* Education, training, and supervision.
* Plan and implement protection such as password software, Multiple Factor Authentication (MFA), and zero trust security.
* Cloud based storage may not protect you.
* Purchase insurance protection to mitigate losses! At a minimum, can provide expert assistance in a loss scenario and legal defense if needed.

Cyber security information outlined above is general in nature and is intended to educate & foster discussion in this area. The information provided is an overview of situations and conditions as understood by us. It should not be considered advice, as it may not be timely and could contain inaccuracies or misinterpretations. This information is not intended to be a description of any specific situation or solution. We recommend seeking competent professional cyber security guidance for your particular business. \* Figures are difficult to quantify, as some studies show averages in the millions!