# COVID-19 Update

**RiskPoint Insurance Advisors - Friday, March 20, 2020 – (971) 282- 4304**

**Special points of interest:**

- Emails impersonating the World Health Organization (WHO) are more common
- 80% of Ransomware attacks came from Remote Desktop Protocol (RDP)
- Options for Free Cyber Training should be utilized

## Cyber Risks—New Risks Associated with COVID-19

In these unprecedented times, we wanted to let you know that RiskPoint is still operating business as usual and are here to help. If you need anything at all or have any questions or concerns surrounding Cyber or COVID- 19, please do not hesitate to reach out! We want to provide you with meaningful information regarding the how COVID-19 is increasing opportunities for Cyber Criminals and some recommendations for bolstering security for your business.

CFC is one of the global leaders in providing cyber liability insurance. CFC's in-house cyber incident response team notes, that the public concern about the virus's spread as well as remote working are creating opportunities for cybercriminals. This advisory provides some background on these risks along with some easy-to-implement steps that businesses can follow to avoid falling victim.

As new cases of the Coronavirus continue to be reported daily, cybercriminals have been leveraging the situation to take advantage of those looking for information on the outbreak. Scams include the following and are changing each day:

- The Sophos Security Team has spotted emails impersonating the World Health Organization (WHO). The emails ask victims to "click on the button below to download Safety Measure". Users are then asked to verify their email by entering their credentials, redirecting those who fall for the scam to the legitimate WHO page, and delivering their credentials straight to the phisher.
- Interpol has warned of a large increase in fraudulent websites claiming to sell masks, medical supplies and other high demand items that simply take money from victims and never deliver the promised goods. It is advisable that internet users purchase items only from established and reputable sources.
- There have been reports of airlines and travel companies being impersonated by fraudsters in a bid to either obtain sensitive information, like passport numbers, or install malware on victims' computers. They may say they want to advise you of COVID-19 infected passengers on past flights you've taken or offer discounts on future flights. When in doubt, we advise users to be vigilant when clicking on any links, delete any suspicious emails, and not disclose sensitive information if you are approached unexpectedly.

## Recommendations

We suggest implementing the following steps to bolster security:

### Test remote log-in capabilities

Not only should personal devices be configured for secure remote working, but business should ensure that multi-factor authentication (MFA) is set up immediately. MFA is an authentication process that requires more than just a password to protect an email account or digital identity and is used to ensure that a person is who they say they are by requiring a minimum of two pieces of unique data that corroborates their identity. Implementing this significantly reduces the chances of cybercriminals being able to log into a business's RDP. For more information on MFA and how to implement it, click here.

### Train your employees on how to spot a phishing email

Some policies have free access to a range of risk management tools. We encourage you to reach out if you have questions on what type of tools you have for free. Additionally, some companies are providing training in this time for free. Cyber Risk Aware is providing free training, click here.

### Prepare for operations disruption in advance

Simply put, prepare for the worst. As with so many cyber incidents, time is of the essence so ensure you have an incident response plan in place, if you need a template please contact your advisor and we will provide you one.