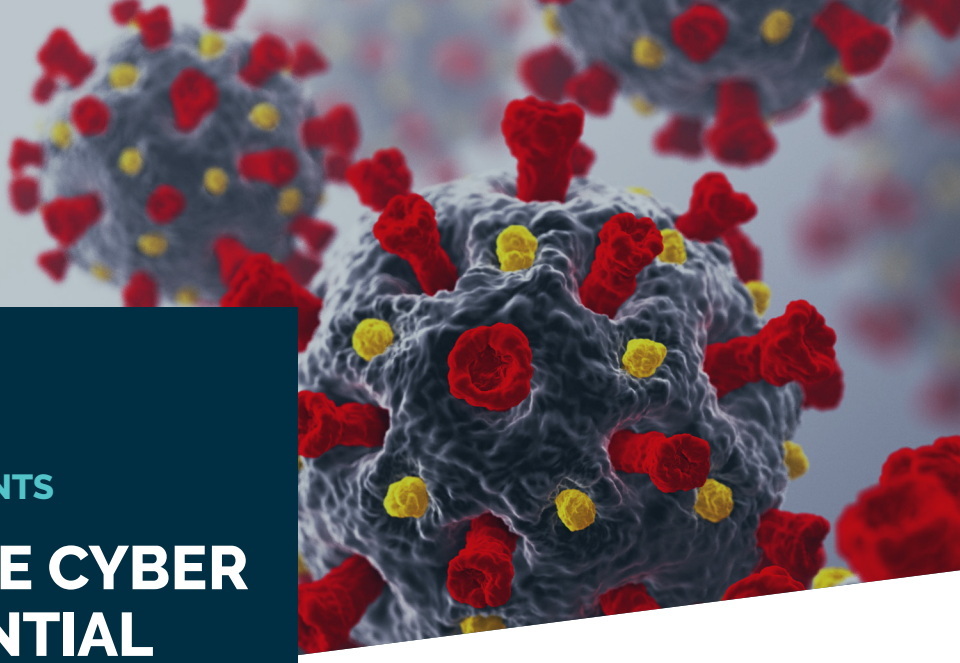

COVID-19 RESOURCES FOR CLIENTS

PANDEMIC DISEASE CYBER INSURANCE POTENTIAL COVERAGE OVERVIEW

There continue to be unknowns regarding the recent outbreak of the coronavirus disease 2019 (COVID-19), and it is important to ensure your business has taken precautionary steps to shield itself from potential cyber liability exposures that could arise. As of today, we are still uncertain of how insurance will respond to COVID-19 related matters. With that said, we feel it is crucial for all enterprises to be aware of the current exposures your enterprise could face to assess all risk management strategies and solutions.

The World Health Organization has declared the spread of COVID-19 a pandemic and the Federal Government has declared a state of emergency. We advise clients to regularly check the Centers for Disease Control and Prevention for proper disease updates and considerations.

When it comes to evaluating your company's exposure to COVID-19 related losses, we advise clients to evaluate their prearranged business continuity plans and inquire further about your current risk transfer solutions.

While it's unlikely that a cyber policy would be triggered due to direct COVID-19 claim there are other things to consider with respect to a company's risk to the spread of the coronavirus:

- **Working from Home** – As the virus spreads and more companies advise their workforce to work from home, employees should stay vigilant when it comes to opening emails and attachments from unknown sources.
- **Fraudulent Wires** – Fraudsters are taking advantage of employees that are working from home especially with requests to change wire information. Be aware that fraudsters are following up an email request to change wire information with a phone call in an attempt to authenticate their fraudulent request.
- **Insurance-Specific Scams** – There is a potential increase of insurance-specific scams posing as solutions to dealing with risks coming from COVID-19. Companies should contact their insurance broker prior to changing terms of current policies.

Alliant

- **IT Security** – With a rise in phishing emails posing as COVID-19 alerts, it is not only important for employees to be aware and be cautious, but equally important for a company's security enterprise teams (either in-house or outsourced) to be up- to-date with antivirus and monitoring tools. Security teams are now dealing with a workforce using personal computers, which can be a weak point compared to enterprise level computers.
- **Business Continuity** – IT infrastructure is now under the burden of the increase in traffic work-from-home employees accessing virtual private networks (VPNs) and other remote log-in capabilities. Companies should have comprehensive incident response and business continuity plans in place that have been tested.

Cyber Insurance may have a more direct role to play in the challenges of current business operations changes due to COVID-19 in the event of a network disruption, where a cyber policy can cover business interruption losses (both direct and contingent) and computer forensics costs associated with investigating a network outage or deterioration of operability.

Should you have any questions or concerns, **please engage your local Alliant contact immediately** or you can visit:

https://insurance.alliant.com/SpecialtyCOVID19-questions

