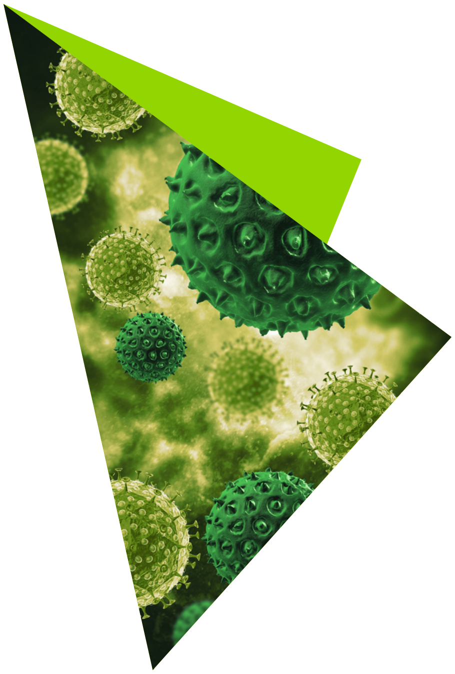

Protecting an Organization's Cybersecurity Posture in Light of Major Health Events

The recent arrival of the Coronavirus (COVID-19) on the world stage has reminded organizations of the potential impact to operations of any pandemic. These operational impacts can have cascading effects on a number of other areas, including cybersecurity. This paper provides advice to our clients on the risks and potential impacts that COVID can have on their cybersecurity posture and provides recommendations for protecting their most critical assets: people, data and networks, processes, systems, and workforce.

As your organization looks for ways to protect your employees from the virus, you may encourage employees to telecommute. Telecommuting minimizes the risk of physically spreading germs but may increase the likelihood of cybersecurity threats for those accessing an organization's systems and applications away from the workplace location. As staff cope with a reduced workforce related to individuals falling ill in their work environment, they may bypass standard security practices and do whatever is necessary to get the job done.

Now is the time to remind your employees to be extra vigilant of your company's cybersecurity policies and protocols. Additionally, it is recommended remind employees how to respond to potentially malicious or suspicious activity. Listed below are the best practices we suggest for employees in their day-to-day business operations.

- **Use corporate email accounts and assets for company business.** The use of personal accounts (e.g., Gmail) exposes an organization's proprietary data to other networks and makes them susceptible to exploitation.
- **Connect to your organization's network through a Virtual Private Network (VPN).** A VPN creates a more secure connection to company systems when operating over a public Internet connection.
- **Read emails carefully.** If something looks suspicious (e.g., typos, asking for personal or financial information), be prudent and report and forward the message to your security team.
- **Exercise caution** with suspicious emails and texts encouraging you to click on links to receive updated company guidance on coronavirus, etc. Validation of these messages can prevent an organization from spending millions of dollars to respond to a breach.
- **Update passwords** and perform device software updates, as advised.

If you should need advice and support, Guidehouse has a robust cybersecurity practice that provides services to all levels of an organization. For more information, contact Marianne Bailey, Guidehouse Advanced Solutions, Cybersecurity Lead, at mbailey@guidehouse.com.

Email: cybersecurity@guidehouse.com / **Web:** guidehouse.com / @guidehouse / linkedin.com/company/guidehouse