County Risk Sharing Authority
a service program of the County Commissioners Association of Ohio

209 East State Street • Columbus, Ohio 43215-4309
Phone: 614-221-5627 • Fax: 614-220-0209
Toll Free: 888-757-1904 • www.corsa.org
Claims Unit Toll Free: 866-455-8039

RISK CONTROL SERVICE BULLETIN

REMOTE WORK CYBERSECURITY

As appointing authorities modify operations, including limitation of hours and services, in response to COVID-19, attention must be given to increased cyberthreats. Networks will be strained, and there will be a greater number of cyberattacks, as well as phishing and social engineering campaigns. While remote working may help reduce the spread of COVID-19, it presents cybersecurity challenges that must be considered before increasing the number of employees that work remotely. Below is a non-exhaustive list of general cybersecurity considerations:

1. *Most important*, work with your IT department or service providers regarding remote work to ensure secure and efficient operations based on your unique systems;
2. Implement and enforce two factor authentication;
3. Have a policy that establishes remote work guidelines that includes access to the county/appointing authority's system with security protocols;
4. Identify employment positions that are able to work remotely and limit access to only systems and information necessary to perform individual job duties;
5. Communicate suspected data breach protocol;
6. Train employees on remote work, phishing, document and other forms of social engineering;
7. Inventory sensitive information/documents (e.g. HIPAA) and ensure security software and protocols are in place (e.g. VPNs, encryption, blockchain…) CORSA members can take advantage of CORSA U Cybersecurity Training. Questions regarding CORSA U can be directed to Jim Hale, CORSA Loss Control Coordinator at: jhale@ccao.org;
8. Do not allow sharing of work computers & communication devices;
9. "Remember password" function should be turned off;
10. Test remote access capacity/increased capacity;
11. Consult reliable sources such as the Cybersecurity and Infrastructure Security Agency (CISA) Attached please find CISA's Risk Management for COVID-19);
12. If employees are permitted to use personal computers to work remotely, appointing authorities should ensure that personal computers have valid up to date anti-virus software and fire walls.

This Risk Control Bulletin is intended to provide general cybersecurity considerations and is not a replacement for your IT department or provider. Should you have questions regarding this Bulletin or CORSA Risk Management services please contact Frank Hatfield, CORSA Risk Control Manager, at (614) 560-1474 or fhatfield@ccao.org

March 16, 2020

CISA
CYBER+INFRASTRUCTURE

March 6, 2020

CISA INSIGHTS

Risk Management for Novel Coronavirus (COVID-19)

The Threat and How to Think About It

This product is for executives to help them think through physical, supply chain, and cybersecurity issues that may arise from the spread of Novel Coronavirus, or COVID-19. According to the U.S. Centers for Disease Control and Prevention (CDC), COVID-19 has been detected in locations around the world, including multiple areas throughout the U.S. This is a rapidly evolving situation and for more information, visit the CDC's COVID-19 Situation Summary.

COVID-19 Risk Profile

As of March 2020, the CDC notes that most people in the United States have little immediate risk of exposure to this virus. The virus is NOT currently spreading widely in the United States.

In anticipation of a broader spread of COVID-19, globally and within the United States, organizations should plan for potential impacts to their workforce and operations.

CISA's Role as the Nation's Risk Advisor

The Cybersecurity and Infrastructure Security Agency (CISA) is working closely with partners to prepare for possible impacts of a COVID-19 outbreak in the United States. COVID-19 containment and mitigation strategies will rely heavily on healthcare professionals and first responders detecting and notifying government officials of occurrences.

CISA will use its relationships with interagency and industry partners to facilitate greater communication, coordination, prioritization and information-sharing between the private sector and the government.

As the situation changes, the virus may affect essential operations for businesses and federal, state, local, tribal, and territorial (SLTT) government entities.

To stay current with CISA's efforts regarding the COVID-19, visit: cisa.gov/coronavirus.

What's in this guide:

Additional Information:

Visit the CDC website, or contact CDC for COVID-19-related issues or to share critical and timely information by sending an email to eocjiclead2@cdc.gov and eocjictriage2@cdc.gov or by calling 1-800-232-4636.

Actions for Infrastructure Protection

Planning and preparedness are critical to reducing the impact of COVID-19 on the Critical Infrastructure community and CISA recommends organizations take the following precautions to prepare for possible impacts from COVID-19:

- **Designate** a response coordinator and assign team members with specific responsibilities.
- **Implement** a formal worker and workplace protection strategy.
- **Train** workers on personal and worksite protection strategies.
- **Establish** and test flexible worksite (e.g., telework) and work hour policies.
- **Identify** essential functions, goods, and services your organization requires to sustain its own operations and mission.
- **Determine** how long your organization can expect to continue providing essential functions, goods, and services in potentially reduced quantities.
- **Identify and prioritize** suppliers of critical products and services for your organization.
- **Continuously assess** ongoing preparedness activities to adjust objectives, effects, and actions based on changes in the business and greater economic and social environments.
- **Monitor** federal, state, local, tribal and territorial COVID-19 information sites for up-to-date information on containment and mitigation strategies.

Actions for your Supply Chain

- **Assess** your organization's supply chain for potential impacts from disruption of transport logistics and international manufacturing slowdowns resulting from COVID-19.
- **Discuss** with those suppliers any challenges they may be facing or may expect to face due to the ongoing situation.
- **Identify** potential alternate sources of supply, substitute products, and/or conservation measures to mitigate disruptions.
- **Communicate** with key customers to keep them informed of any issues you have identified and the steps you are taking to mitigate them.

Cybersecurity for Organizations

As organizations explore various alternate workplace options in response to COVID-19, CISA recommends examining the security of information technology systems by taking the following steps:

- Secure systems that enable remote access.
  - » **Ensure** Virtual Private Network and other remote access systems are fully patched.
  - » **Enhance** system monitoring to receive early detection and alerts on abnormal activity.
  - » **Implement** multi-factor authentication.
  - » **Ensure** all machines have properly configured firewalls, as well as anti-malware and intrusion prevention software installed.
- **Test** remote access solutions capacity or increase capacity.
- **Ensure** continuity of operations plans or business continuity plans are up to date.
- **Increase** awareness of information technology support mechanisms for employees who work remotely.
- **Update** incident response plans to consider workforce changes in a distributed environment.

Cybersecurity Actions for your Workforce and Consumers

Malicious cyber actors could take advantage of public concern surrounding COVID-19 by conducting phishing attacks and disinformation campaigns. Phishing attacks often use a combination of email and bogus websites to trick victims into revealing sensitive information. Disinformation campaigns can spread discord, manipulate the public conversation, influence policy development, or disrupt markets.

CISA encourages individuals to guard against COVID-19-related phishing attacks and disinformation campaigns by taking the following precautions:

- **Avoid** clicking on links in unsolicited emails and be wary of email attachments.
- **Do not reveal** personal or financial information in emails, and do not respond to email solicitations for this information.
- **Review** CISA's Tip on Avoiding Social Engineering and Phishing Scams for more information on recognizing and protecting against phishing.
- **Review** the Federal Trade Commission's blog post on coronavirus scams for information on avoiding COVID-19 related scams.
- **Use** trusted sources—such as legitimate, government websites—for up-to-date, fact-based information about COVID-19.