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

On March 11, the COVID-19 outbreak was characterized as a pandemic by the WHO. The virus that causes COVID-19 is infecting people and spreading easily from person-to-person. Cases have been detected in most countries worldwide and community spread is being detected in a growing number of countries.

In anticipation of a broader spread of COVID-19, globally and within the United States, organizations should plan for continued 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:

- Actions for Infrastructure Protection
- Actions for your Supply Chain
- Cybersecurity for Organizations
- Cybersecurity Actions for your Workforce and Consumers

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.