CISA ROLE

Risk Management during COVID-19

Best Practices
We are the Nation’s Risk Advisors

CISA leads national risk management for cyber and physical infrastructure
CISA mission: Lead the collaborative national effort to strengthen the security and resilience of America’s critical infrastructure

In support of that mission, Cybersecurity Advisors (CSAs):

- **Assess:** Evaluate critical infrastructure cyber risk.
- **Promote:** Encourage best practices and risk mitigation strategies.
- **Build:** Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate:** Inform and raise awareness.
- **Listen:** Collect stakeholder requirements.
- **Coordinate:** Bring together incident support and lessons learned.
CISA Insights – 18 MAR 2020

• Risk Management for Novel Coronavirus (COVID-19)

• 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.

• What’s in this guide:
  • Actions for Infrastructure Protection
  • Actions for your Supply Chain
  • Cybersecurity for Organizations
  • Cybersecurity Actions for your Workforce and Consumers

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

CISA Insights – 18 MAR 2020

• 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.

• 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
Most Common Cyber Threats

- Ransomware
- Phishing Campaigns & Business E-mail Compromise
- Lack of Software Patching
- Misconfiguration of Technology
- Supply Chain (Hardware, Software, Cloud Services)
- Advanced Persistent Threats (Organized, Well-funded, Highly-capable Groups)
- Internet of Things (IoT)
- Insider Threats (Intentional & Unintentional)
- Weak Passwords

*These threats increase the likelihood of a compromise.

BEST PRACTICES

MAKE YOUR OWN LUCK!

- Leadership Must OWN the Issue
- Be Prepared – EXERCISE
- Good Cyber Hygiene – Blocking and Tackling
- Defend and Continue to Operate
- Leverage Relationships
QUESTIONS?

Contact Us

Ron Ford
DHS/CISA Cybersecurity Advisor
Region 1 - New England
Ron.Ford@cisa.dhs.gov
cyberadvisor@cisa.dhs.gov
www.cisa.gov/cybersecurity

Report Cyber Incidents:

DHS/CISA
24/7 Line: 888-282-0870
CISAServiceDesk@cisa.dhs.gov
https://www.us-cert.gov/report

MS-ISAC
https://www.cisecurity.org/ms-isac/
24/7 Line: 866-787-4722
soc@cisecurity.org
https://www.cisecurity.org/isac/report-an-incident/