Resources – Ransomware Work Project

The resources below are provided by the PRIA Ransomware Work Project.

Government Websites

[Department of Homeland Security]

Created in 2018, the Cybersecurity Infrastructure Security Agency (CISA) operates under the auspices of the Department of Homeland Security and is the nation's risk advisor, working with partners to defend against today's threats and collaborating to build a more secure and resilient infrastructure for the future.

CISA, in conjunction with its sister agency, the National Cybersecurity and Communications Center (NCCIC), provides extensive cybersecurity and infrastructure security knowledge and practices to its stakeholders, shares that knowledge to enable better risk management, and puts it into practice to protect the nation's essential resources.

Together, the CISA & NCCIC are a global exchange for cyber and communications information, sharing what they receive back to the cybersecurity community.

[Cybersecurity and Infrastructure Security Agency (CISA)]

Cybersecurity and Infrastructure Security Agency (CISA) is a resource to defend against cyberattacks and works with critical infrastructure owners and operators, including state, local, tribal and territorial partners, to provide cybersecurity tools, incident response services and assessment capabilities to safeguard the '.gov' networks that support the essential operations of partner departments and agencies.

CISA coordinates security and resilience efforts using trusted partnerships across the private and public sectors, and delivers technical assistance and assessments to federal stakeholders as well as to infrastructure owners and operators nationwide.

They are a multi-tiered organization that coordinates security and resilience efforts, providing a robust offering of cybersecurity and critical infrastructure training opportunities and facilitate an information-sharing environment for government.

CISA – Ransomware Guidance and Resources

Learn more about the growing cyber threat. With industry best practices and individualized checklists, the new Ransomware Guide is a starting place. The guide, released in September 2020, represents a joint effort between CISA and the Multi-State Information Sharing and Analysis Center (MS-ISAC). The joint Ransomware Guide is a customer-centered, one-stop resource with best practices and ways to prevent, protect and/or respond to a ransomware attack.

Training Program

The Federal Virtual Training Environment (FedVTE) provides free online cybersecurity training to federal, state, local, tribal, and territorial government employees, federal contractors, and US military veterans.

Incident Response publication

This National Institute of Standards and Technology (NIST) publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. Topics covered include organizing a computer security incident response capability, handling incidents from initial preparation through the post-incident lessons learned phase, and handling specific types of incidents.

Technical Guidelines

Guidelines providing technical requirements for federal agencies implementing digital identity services, which are not intended to constrain the development or use of standards outside of this purpose. The guidelines cover identity proofing and authentication of users (such as employees, contractors, or private individuals) interacting with government IT systems over open networks.

Public Awareness Campaign

The STOP.THINK.CONNECT.™ Campaign is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. When we all take simple steps to be safer online, it makes using the Internet a more secure experience for everyone.

Protection against Ransomware Attacks

Ransomware can be devastating to an individual or an organization. Anyone with important data stored on their computer or network is at risk, including government or law enforcement agencies, healthcare systems or other critical infrastructure entities. Recovery can be a difficult process that may require the services of a reputable data recovery specialist, and some victims pay to recover their files; however, there is no guarantee that individuals will recover their files if they pay the ransom.

CISA offers recommendations to protect users against the threat of ransomware.

Business Websites

State-by-State Map of Incidents

This site provides a regularly updated listing, by state, of cyberattacks. The data available for each incident seems to be minimal, but it is current. The company, SecuLore, is a cybersecurity company with expertise in public safety (the 911 Centers). A one-size-fits-all cybersecurity solution is not effective because open communication with the public is a necessity. Their mission is to empower public safety professionals and their IT teams so that they can continue to aid the public knowing that they are cyber-protected.

The State of Ransomware in the US: Report and Statistics December 2019

In 2019, the U.S. was hit by an unprecedented and unrelenting barrage of ransomware attacks that impacted at least 966 government agencies, educational establishments and healthcare providers at a potential cost in excess of $7.5 billion. This report summarizes the extent of the ransomware impact in the United States.

Training Platform

An integrated cybersecurity training platform for security awareness training combined with simulated phishing attacks to manage the continuing problem of social engineering.

PRIA Member-provided Resources

(If you have resources to add to this list, contact the PRIA office.)

Ransomware Survival Guide

It is important that your organization be prepared to confidently respond to, and survive, a ransomware attack. This survival guide will arm you with the knowledge you need to defend against and prepare for an attack.

Ransomware Checklist

The key to successfully responding to and managing incidents is a comprehensive and rehearsed incident response program. This Ransomware Incident Response Checklist will provide you with an outline of the key steps needed to help your organization prepare for a ransomware attack - including preparation, analysis, mitigation, and wrap-up.