NGA Cybersecurity Newsletter

June 2, 2020
Contact: John Guerriero (jguerriero@nga.org)
202-624-5372

Resource Center Announcements

NGA Webinar: Exercising Enterprise Security in a Remote Environment – June 17, 2020 from 1 – 2pm

Please join NGA on **June 17th from 1:00 – 2:00pm Eastern** to hear from leading industry experts on *Exercising Enterprise Security in a Remote Environment*. The global pandemic shines a spotlight on the importance of enterprise risk management (ERM) as well as business continuity, disaster recovery and crisis management. With many organizations rapidly shifting to a work-from-home model — and exposing themselves to new security threats in the process— it's clear that security and risk management leaders need a more prominent role in shaping enterprise risk management strategies.

Please register for the webinar here.

May Webinar: Virtual Upskilling Opportunities in Cybersecurity

The NGA Resource Center for State Cybersecurity held a webinar on May 13, 2020 on Virtual Upskilling Opportunities in Cybersecurity. The webinar featured panelists from CompTIA, the Purdue University Cybersecurity Apprenticeship Program, NICE, and the Missouri Office of Workforce Development and explored how states can take advantage of virtual programs to upskill their workforce, especially as they look to make an economic recovery. Please access slides here and a recording of the webinar here.

NGA Request for Information:

1. What creative public-private partnerships has your state leveraged to add to its existing federal and state funding sources for cybersecurity?

2. How has your state worked to reduce overall risk to local governments? Have there been certain authorities, incentives, and/or regulations that have had a significant impact?

3. Has your state assumed responsibility for local governments' cyber preparedness programs? If so, what services are provided?

Please reach out to John Guerriero here on the above requests.

Cybersecurity Resources

PTI Webinar: Broadband Capacity and Availability in a Crisis

CompTIA's Public Technology Institute (PTI) is hosting a webinar series exploring cybersecurity, emerging technologies and other issues facing local government tech leaders around the country in these uncertain and challenging times. On **June 4 from 2:00 – 3:00pm ET**, PTI will be hosting a webinar on *Stretching the Limits: Broadband Capacity and Availability in a Crisis*. This is one in a series of six webinars presented by PTI in association with NGA, the National League of Cities, and NASCIO. Visit the PTI Webinar Series webpage here to register and access on demand.

CISA Releases Cyber Essentials Toolkit

DHS' Cybersecurity and Infrastructure Agency (CISA) released the first in a series of six toolkits supporting its 2019 Cyber Essentials guide. The toolkit breaks down the Cyber Essentials into action items for IT and C-suite leadership. Read more about CISA's Cyber Essentials here and access Toolkit 1 here.

Secure Video Conferencing Recommendations for Schools

As use of video conferencing platforms becomes more embedded in school environments, CISA released a list of recommendations for school districts and IT administrators to help secure school networks. Access the recommendations here and CISA's tips for students and staff safe here.

GAO Calls for Federal Agencies to Align Cyber Standards with States

The General Accountability Office (GAO) urged federal agencies to streamline the different cybersecurity standards that states using federal data are required to meet. The GAO report makes recommendations for federal agencies to harmonize their regulations and make compliance less burdensome for states. Read more about the report and its highlights and recommendations here.

FISMA Report Shows Cyber Compliance Improvement in Federal Agencies

The White House released its annual Federal Information Security Management Act (FISMA) report to Congress. The report states that 72 agencies received the "Managing Risk" rating in FY 2019, up from 62 in FY 2018. Agencies reported an 8% decrease in cybersecurity incidents in 2019. The report also noted that while 100% of the agencies established rules of behavior for handling federal information and consequences for violation, only 58% had implemented policies to hold contractors to the same standards. Read more about the report here, and read the report here.

Securing IOT Devices

The Center for Internet Security (CIS) released a brief guide and recommendations for securing smart devices and protecting one's privacy. The recommendations include updating passwords and default settings, implementing patches, and using multi-factor authentication. See the guide here.

NASCIO Mid-year 2020 Conference Resources

NASCIO held a series of virtual sessions in early May in lieu of its in-person conference. The sessions discussed a variety of topics, including state-local partnerships and the effect COVID-19 is having on state networks. You can access recordings of the sessions here.

Election Security Resources

Election Administration Costs Outpace Federal Funding

The Alliance for Securing Democracy released a report outlining how COVID-19 is affecting the costs and needs for state and local election administrations. The report finds that the $400 million allocated by Congress in March covers only a fraction of what is needed to run elections during a pandemic, especially considering vote-by-mail expansion, public education campaigns, and the provision of protective equipment. Read the report here.

Federal Agencies Warn of Significant Cyber Risks of Online Voting

In a memo to state election officials and vendors, CISA and other federal agencies expressed their concern over the security risks posed by online voting. The guidance warns that ballots returned online are vulnerable to disruption and could be manipulated at scale by hackers. The FBI, Election Assistance Commission (EAC) and National Institute of Standards and Technology (NIST) joined CISA in signing off on the document. Read more here.

EAC Announces HAVA Funds Available to States Until Expended

The EAC notified states that the five-year limitation on the availability of HAVA funds no longer applies, including those funds allotted in 2018 and 2020. Read more about the move here.

Cybersecurity News

State Unemployment Insurance Programs Targeted

The U.S. Secret Service (USSS) reports that a Nigerian fraud ring is exploiting the COVID-19 crisis to launch large-scale fraud campaigns against state unemployment insurance programs. The USSS warns that every state is vulnerable to the scheme and will likely be targeted if it has not already. The group is using U.S. citizens' data – some of which it may have accessed in previous breaches, including social security numbers – to file fraudulent unemployment claims on their behalf, even if they did not lose their job. Read more here. As of release, Washington State has recovered $300 million and blocked the actors from stealing more. Read more here.

U.S. Agencies Issue Joint Alert on COVID-themed Payment Scams

CISA, the Department of Treasury, Internal Revenue Service, and U.S. Secret Service issued a joint alert with mitigations to help the public avoid scams related to the COVID-19 relief payments. Read the joint alert here.

Alert Issued Regarding North Korean Malware

CISA, the FBI and Department of Defense (DOD) released three alerts relating to malware variants used by the North Korean government. The alerts offer an analysis of the tools and infrastructure used, description of the malware, and suggested response and mitigation actions. Read the alerts here.

Minneapolis City Government Sites Hit by DDoS Attack

City government systems in Minneapolis were hit by several distributed denial of service (DDoS) attacks. One attack temporarily made down several public websites inaccessible while another attack against state computer systems was less effective. The attack comes as the nation faces ongoing protests over the death of George Floyd. Read more here.

COVID-19 Research Industry Targeted by Cyber Actors

CISA and the FBI released an alert raising awareness to the threat facing organizations conducting COVID-related research. Threat actors, including those affiliated with the People's Republic of China, are looking to obtain intellectual property and public health information regarding potential vaccines, treatment, and testing. The alert urges these organizations to maintain dedicated cybersecurity and insider threat practices to protect the integrity of the data. Read the alert here.

In the wake of alert, Congress has requested briefings from CISA and the FBI on the threat facing U.S. research organizations. Read more here.

Arkansas Establishes Panel to Review Contact Tracing Technology

Arkansas Governor Asa Hutchinson created a panel to review any technologies that the state may use as it develops a contact tracing program. The 12-member program includes the state CISO, chief privacy officer, and deputy chief data officer. Read more here.

New York Develops Playbook for Developing Public-Private Partnerships

At the onset of the coronavirus pandemic, the New York State Office of Information Technology Services and Department of Financial Services established a Technology SWAT team to assist the state in securing pro bono partnerships with the private sector. The state has released a playbook designed to help other public sector entities looking to establish similar bodies. Read more here.

Ransomware Targets Europe’s Largest Private Hospital Operator

The largest private hospital operator, the Fresenius Group, was hit by a ransomware attack on its technology systems. The attack was part of a larger campaign across Europe deploying the Snake ransomware. Read more here.

COVID Mis- & Disinformation News

CISA Guidance on Misleading Information

CISA released a guide for identifying false and misleading information related to COVID-19, including those pertaining to the virus’ origin, its scale, how it relates to 5G technology, the government’s response to it, and prevention and treatment. Read the full advisory here.

Twitter Adds Feature Flagging False Information, Prompts White House Executive Order

Twitter added a feature that labels misleading, disputed, or unverified tweets relating to COVID-19 and removes those that it believes may lead to harm. The label warns users about the tweets and points them toward authoritative sources like public health organizations and agencies. Tweets whose content may pose a risk to users’ health may be removed from the platform. Read more about the function here.

Twitter added fact checking labels to two of President Trump’s tweets on mail-in voting, marking them as misleading. Afterwards, President Trump issued an executive order aiming to limit the legal protections that offer social media websites immunity from lawsuits. The order requests the Federal Communications Commission to issue a rule clarifying exceptions in Section 230 of the Communications Decency Act, which protects intermediary website operators from libel lawsuits. Read more about the order here, and access the order here.

Study Suggests Many YouTube COVID Videos Contain False Information

A recent study conducted by BMJ Global Health suggests that more than a quarter of the most-viewed coronavirus videos on YouTube contain misleading or inaccurate information. The study also identified methods government agencies can employ to increase viewership of their quality content. Read more here.

Significant Amount of Twitter Accounts Pushing for Reopening Country May be Bots

Researchers at Carnegie Mellon University have discovered that much of the discussion around COVID-19, especially on rescinding stay-at-home orders, is driven by Twitter bots. The research team is seeing more bot activity than predicted and have identified more than 100 types of false COVID-19 stories. Read more here.

NSA Accuses Russian Actors of Attack on Email Servers

The National Security Agency (NSA) reported that a team of Russian cyber actors from its military intelligence unit, the GRU, have been exploiting unpatched vulnerabilities in Exim mail transfer system since August 2019. Read more here.

UTSA Unveils New Cybersecurity Manufacturing Institute

The U.S. Department of Energy selected the University of Texas at San Antonio (UTSA) to establish and lead the Cybersecurity Manufacturing Innovation Institute. As automation increases, cybersecurity is becoming a major concern for manufacturers, including those producing energy technologies. The institute will focus on securing automation and the supply chain network and building a national program for education and workforce development. Read more here.

NGA Government Relations Updates

Bipartisan Congressional Coalition Urges for Future Relief Packages to Include Funding for Modernized State IT Infrastructure

A bipartisan coalition, led by Rep. Jim Langevin (D-RI) and Rep. Michael McCaul (R-TX), requested funding in future COVID relief packages to help modernize and secure state and local government IT infrastructure. The letter was signed by 27 other Representatives and sent to House and Senate leadership. Read the letter here.

Endless Frontiers Act Introduced in Senate

The bill, introduced by a group of bipartisan Senators led by Minority Leader Charles Schumer (D-NY), would create a Directorate of Technology at the National Science Foundation and invest $100 billion over five years in science and technology research, including cybersecurity, AI, and national disaster prevention. Read the bill text here.

NGA Resource Center for State Cybersecurity Partners

- Amazon Web Services
- American Electric Power
- AT&T
- CompTIA
- Deloitte
- Proofpoint
- Rapid7
- Splunk
- Tenable
- VMware