


NGA Cybersecurity Newsletter

February 26, 2021

Contact: John Guerriero (jguerriero@nga.org)
202-624-5372


Resource Center Announcements

NGA 2021 Policy Academy on State Cybersecurity

NGA is pleased to offer states a technical assistance opportunity:  [NGA Policy Academy to Advance Whole-of-State Cybersecurity](#). Selected states will receive hands-on technical assistance from the NGA Resource Center for State Cybersecurity, including two workshops (which can be modularized for the virtual environment). NGA will partner with selected governors' offices to build capacity to address a wide range of objectives in state cybersecurity, including those listed below.

NGA will select up to four (4) states presenting projects around the following strategic priority areas:

- I. Cybersecurity Governance;
- II. Cybersecurity Workforce Development;
- III. Critical Infrastructure Security;
- IV. Local Engagement & Partnership; or
- V. Innovations in State Cybersecurity

Please see the Request for Applications (RFA)  [here](#). For more information, reach out to Maggie Brunner [here](#). Applications are due to Maggie Brunner by **March 5, 2021 at 8pm ET/5pm PT**.

Previous NGA Webinar: Combatting Financial Fraud in State Benefits Program

The NGA Resource Center for State Cybersecurity recently held a webinar on Combatting Financial Fraud in State Benefit Programs. A recording of the webinar is [here](#) (Passcode: \$?P4Y4U&).

NGA Request for Information:

1. Does your state have a cybersecurity or computer science teaching mandate or standards? When formulating teaching content mandates, does your state incorporate national standards and recommendations or depend on local guidance?
2. If your state conducts risk assessments and incident response services for local governments, what role do data and metrics play in performance improvement and budget requests?

3. How is your organization looking to promote a culture of diversity, equity, and inclusion in its cybersecurity workforce?

Please reach out to John Guerriero [here](#) on the above requests.

Cybersecurity Resources

Proofpoint's 2021 State of the Phish Report

Proofpoint released their 7th Annual State of the Phish report that explores the spike in COVID-themed phishing attacks and ransomware incidents. The report features analysis of survey responses, simulated phishing exercises, and real-world attacks to provide insights into phishing and other cyber threats—and what organizations can do about them. Among the report's key findings:

- 98% of infosec professionals surveyed said their organization has a security awareness training program—but only 64% offer formal training sessions as part of their program.
- Two-thirds of survey respondents said their organization experienced a ransomware infection in 2020, and over half paid the ransom.
- Nearly 40% of the respondents who paid a ransom in 2020 were hit with additional demands following an initial payment.

Read the report [here](#).

CIS Guide on Managing Cybersecurity Supply Chain Risks in Election Technology

The Center for Internet Security (CIS) released a new guide for Managing Cybersecurity Supply Chain Risks in Election Technology, a Guide for Election Technology Providers. The guide provides best practices for specific problem areas identified by the election community. It contains recommendations and best practices to address the issue and lays out a holistic, consistent approach to risk management. Read more [here](#).

CrowdStrike 2021 Global Threat Report

CrowdStrike Inc. released their 2021 CrowdStrike Global Threat Report detailing unique insights to the global threat landscape and offering best practices for organizations looking to amplify their cybersecurity maturity in 2021. The report highlights that eCrime attacks made up 79% of all intrusions. The report also includes a new ECrime Index that displays the intensity of cyber-criminal markets over time. Read more [here](#).

CISA and CYBER.ORG Partner to Deliver Cyber Safety Video Series

The Cybersecurity and Infrastructure Security Agency (CISA) and CYBER.ORG announced a video series on cyber safety to help those learning or working remotely take proactive steps to protect themselves and their business. The 5-video series delivers easily understood cybersecurity concepts that are appropriate for all users, not just K-12 educational institutions. More videos are scheduled to be released in the coming months. You can read more [here](#).

NSA Guidance on Zero Trust Security Model

The National Security Agency issued guidance on *Embracing the Zero Trust Security Model*, offering the benefits and challenges associated with the model as well as recommendations for organizations looking to implement it within networks. Read the guidance [here](#).

Cybersecurity Legislation Assessment for 116th Congress

Third Way released a comprehensive analysis of the cybersecurity legislation introduced in the 116th Congress. The report dives into what aspect of cybersecurity the bills focus on, comparisons to the 115th Congress, what gaps remain and how the current Congress can continue to build on the previous work. Read the report [here](#).

NCIJTF Releases Ransomware Factsheet

The National Cyber Investigative Joint Task Force (NCIJTF) released a joint-sealed ransomware factsheet on current ransomware threats, which includes information on prevention and mitigation techniques. The factsheet was developed by subject matter experts from more than 15 government agencies to increase awareness on ransomware threats to police and fire departments; state, local, tribal, and territorial governments; and critical infrastructure entities. You can find the factsheet [here](#).

Ransomware Biggest Threat Facing Higher Ed

Cybersecurity services company BlueVoyant released findings from its Cybersecurity in Higher Education report, which outlines the threat landscape facing the higher ed sector and the impact breaches have on the sector. Key findings include that ransomware is the number one threat facing higher ed institutions and ransomware events doubled from 2019 to 2020. Report lists common vulnerabilities identified in the sector as well as common tactics deployed by threat actors. Read the report [here](#).

Policy Recommendations for the Future of Election Security

Harvard University's Belfer Center for Science and International Affairs has identified four challenges that policymakers and election officials must address to properly invest and reinforce in future elections. The report also highlights key recommendations for how those challenges can be addressed by state and federal legislators and policymakers. Read the report [here](#).

Registration Open for K-12 Cybersecurity Leadership Symposium

The K12 Security Information Exchange (K12 SIX), a new national non-profit dedicated to supporting the cybersecurity of K-12, is hosting a free, half-day virtual conference on the evolving cybersecurity challenges facing the education sector and the innovative strategies needed to mitigate them. Register and view the agenda [here](#).

Improving Inclusion and Equity in Tech through Apprenticeship

The Urban Institute highlighted strategies to improve diversity and inclusion in tech jobs through the expansion of tech apprentice programs. While tech apprenticeship programs offer non-traditional pathways to quality jobs and benefit the organizations implementing them, programs can strive to ensure that apprentices see themselves represented throughout the organization. You can read more [here](#).

Cybersecurity News

Washington State Senate Passes Bill to Strengthen Cybersecurity After Breach

Following an unemployment-claims data breach that exposed the personal information of 1.4 million people in Washington State, the Washington state Senate unanimously passed legislation to give more authority to the Office of Cybersecurity (OCS). The legislation, a request from Governor Inslee, would give OCS more authority to safely store sensitive data, centralize operations, and formalize some of the authorities that already exist within the agency. It will also require WaTech and the Attorney General's office to research best practices for data collection and submit a report to the legislature.

The bill now moves to the state House for further consideration. You can see the bill's text [here](#) and read more about the legislative push in Washington and around the country [here](#) and [here](#).

Florida Water Treatment Facility Compromised

The city of Oldsmar, FL experienced a cyberattack where an unidentified hacker gained remote access to a drinking water treatment facility's supervisory control and data acquisition (SCADA) system. CISA and the FBI released a threat advisory that claims the actor(s) behind the attack gained access by exploiting cybersecurity weaknesses, including weak passwords and outdated operating systems. The advisory offers a threat overview of desktop sharing software and Windows 7 end of life while also offering recommendations for mitigation and prevention. Read the CISA and FBI advisory [here](#).

Federal Discussions on SolarWinds Cleanup

The Senate Intelligence Committee held a hearing on the SolarWinds attack and its continuing impact this week. Senators and corporate executives stated that the scope and scale of the operation were unclear and the attack may still be continuing. Listen to the hearing [here](#).

On February 17, Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger stressed that it will take a while to sort through the fallout from the SolarWinds security breach earlier this year. Currently, nine federal agencies and approximately 100 private sector entities were compromised in the suspected Russian hack of the SolarWinds network management software update. Read more [here](#).

DHS Announced Steps to Advance the President's Cybersecurity Commitment

DHS Secretary Mayorkas recently announced how the department will act on President Biden's vision to elevate cybersecurity across the federal government. The Department will continue to lead efforts on risk mitigation, strengthen private sector partnerships and look to increase the required minimum spend on cybersecurity through FEMA grant awards. Read more [here](#).

Ohio Cyber Reserve Deployed in Incident Response

A member of the Ohio Cyber Reserve was deployed on state active duty under Governor DeWine's authority to assist a government agency mitigate a cybersecurity breach. This marks the first time a member of the Ohio Cyber Reserve has been deployed since the unit was established by the passage of Senate Bill 52. Read more [here](#).

Governor Mills Establishes Cybersecurity Advisory Council

Maine Governor Janet Mills issued an executive order establishing the State of Maine Cybersecurity Council to strengthen the security and resiliency of the state's IT infrastructure and ensure an effective communication chain to the Governor's office. Among the items the Council will look to address are formalizing strategic partnerships at the state and federal level, cybersecurity workforce development and incident response and risk management. Read the Executive Order [here](#).

New York Issues Cybersecurity Insurance Risk Framework

The New York State Department of Financial Services (DFS) released a framework outlining industry best practices for state-regulated property/casualty insurers that write cyber insurance to help them manage cyber insurance risk. DFS advises those property/casualty insurers to establish a formal strategy for measuring cyber insurance risk that incorporates a set of best practices. Read more [here](#).

Kent State University Makes the Leap to Zero Trust Security

Kent State's chief information security officer details in a podcast how he transitioned the university to zero trust security. The podcast talks about gaining buy-in with the university administrators, implementing his strategy, and what lessons other colleges and universities can draw from Kent State's experience. Read more [here](#).

A New Game Teaches Students Cyber Hygiene

The University of Texas at San Antonio Center for Infrastructure Assurance and Security recently launched Cyber Threat Protector, a card game designed to introduce cybersecurity principals to children as young as 8 years old. Read more [here](#).

NGA Government Relations Updates

DHS Increases Share of FEMA Grants to be Spent on Cybersecurity

DHS Secretary Mayorkas announced an increase in the required cybersecurity minimum spend in the FEMA Homeland Security Grant Program in FY21 from 5% to 7.5%. Read the announcement [here](#) and the FY21 HSGP Notice of Funding Opportunity [here](#).
