February 24, 2022

COORDINATION AND EDUCATION KEY TO CYBER READINESS

Recently, national trends have pointed towards a more digitized way of life, including the way our government operates at all levels. The introduction of COVID-19 only accelerated the shift to digital services and, along with that shift, a clear focus on maintaining security at the federal, state, and local levels.

Nevada's Office of Cyber Defense Coordination (OCDC), established pre-pandemic, proves itself a valuable asset to the state as it aims to provide cybersecurity, cyber-hygiene, and improved cyber-education and training.

Established by statute in 2017, the **OCDC's** duties aim at becoming the statewide coordinating entity in Nevada. The primary goals of the Office are to establish relationships with a variety of different organizations – from local subdivisions to educational institutions and the private sector stakeholders. The OCDC also utilized regulatory authority over state executive agencies and political subdivisions to oversee risk assessments and general cyber-strategy across the state.

The flexibility of the Office allows them to maintain an optimized and efficient cybersecurity strategy for the state. As far as oversight, OCDC is an office within the Department of Public Safety (DPS) with annual and quarterly reporting requirements. Their funding comes through the Nevada DPS funding as well, provided through the state's General Fund.

Fast-forwarding to current day, with the pandemic spikes and drops, governments see a more permanent digital future and opportunities to invest in educating their workforce – something OCDC considers to be one of its highest valued specialties. The office coordinates with local governments by engaging with both technical and non-technical local partners; examples include CIOs and CISOs, members of city councils, county and city managers, and other political subdivisions to show the importance of investing in proper cybersecurity strategies.

Along with local governments, the private sector is also adopting a more flexible remote work model and increasing its use of digital services. OCDC sees this shift in the private sector as an opportunity to educate a new sphere of professionals on the importance of maintaining proper cybersecurity. OCDC embraces this public-private partnership by leveraging relationships with small business organizations in the state to get in front of private sector executives and educate them on how they can fortify and protect their systems and operations – some of which are used by political subdivisions.

Outside of providing education and training, OCDC develops partnerships with colleges and universities across the state to continue developing the cyber-workforce and provide outreach services across the state. For example, the **University of Nevada—Reno (UNR), University of Nevada—Las Vegas, and the College of Southern Nevada developed cybersecurity degree programs jointly supported by DHS and the National Security Agency.** Through these programs, the state offers a variety of associate's, bachelor's, and master's programs aimed at increasing the cyber-knowledge of the state's workforce. In addition to their cybersecurity degree programs, UNR established a nationally known Cyber Club. Currently with around 30 students, the club utilizes their academic knowledge and skills to facilitate training opportunities, including providing first-hand training and response practice to members of Nevada's National Guard. This level of preparedness allows the state to better understand incident response before a breach occurs.

OCDC also has a focus on soliciting grants and providing technical training to state and local entities. One example of OCDC successfully securing grants occurred recently, when the Office, in partnership with Nevada's CISO Office, solicited funds from DHS to purchase a bulk order of SANS Institute training vouchers for cybersecurity. Briefly, the SANS Institute technical training programs are a pinnacle of cybersecurity training and vastly increases the knowledge on cybersecurity for its participants. Through securing these vouchers, OCDC was able to provide 50 vouchers to executive branch departments and local entities across the state and allow them to choose their training level and goals – tailoring each training to the county or region that is awarded the voucher.

Administratively, OCDC witnessed several important statute changes in 2019, during Nevada's 80th Legislative Session. Specifically, Senate Bill 69 created numerous improvements to OCDC core competencies, as well as other statewide cybersecurity initiatives. First, several statutes were adjusted to eliminate duplication of effort and improve cybersecurity efficiencies within the State Executive Branch. Further, additional compliance-based mandates were added, which now requires OCDC to serve as the focal point for reporting cybersecurity policy adherence, for executive branch agencies. SB69 also further expanded OCDC's role and protections of private sector entities while investigating cybersecurity incidents.

OCDC is also tasked with the development and continuous improvement of Nevada Administrative Code for regulation of city and county cybersecurity incident response plans. Through this authority, OCDC has successfully established a statewide baseline for cybersecurity incident response plans and reporting.

Shaun Rahmeyer, Administrator for OCDC, emphasizes the need to leverage partnerships and collaboration to secure information technology infrastructure. Rahmeyer says, "The cyber threat landscape continues to shift, and with few mature cybersecurity programs in existence – whether government or private sector – the need for organizations to increase investments in agile and resilient security is paramount. Future efforts to combat the growing cyber threat requires extensive collaboration between stakeholders. The public, business decision-makers, and government officials can no longer afford to discount the cyber threat to their organizations and the community."

I really think that if we change our own approach and thinking about what we have available to us, that is what will unlock our ability to truly excel in security. It's a perspectives exercise. What would it look like if abundance were the reality and not resource constraint?

- Greg York

If you would like more information or have a state practice you'd like to highlight as part of this ongoing series, please contact Jamie Logan

nemaweb.org

NEMA®
NATIONAL EMERGENCY MANAGEMENT ASSOCIATION

NEMA MID-YEAR FORUM
March 28 – 31, 2022
Alexandria, VA