OCIOdoings

July 2020

Information Security Maturity Assessment and Perimeter Penetration Test

LA County worked with a 3rd party consulting organization to perform an information security program maturity assessment and perimeter penetration test. The purpose of which was to help LA County evaluate the security controls across the enterprise which included all 34 County departments, determine maturity state for processes and technologies, as well as identify gaps and risks associated with the organization of information security. The perimeter penetration test results identified and validated vulnerabilities within LA County systems that are susceptible to external attacks. The consulting group also provided LA County with remediation guidance for vulnerabilities and gaps identified as a result of the assessment in the form of a comprehensive cyber security risk management plan and security roadmap. The project team was led by Office of the CIO members Ralph Johnson CISO and Jeffrey Aguilar & Chris Paltao Deputy CISOs.

Cybersecurity Awareness Training

Cybersecurity awareness training is an essential function for an information security program in any organization. All workforce members must be aware of potential threats and information security best practices to reduce the risk of compromise to County workforce members and assets. As an extension to our mandatory cybersecurity awareness training program, we deploy Countywide phishing campaign simulations to have workforce members practice what they learn from their training. Departmental and Countywide phishing campaign simulations are scheduled throughout the year. Our recent COVID-19 themed Countywide phishing campaign simulation was deployed on June 2020. The campaign was active for 2 weeks and all simulated emails were delivered within three days of starting the campaign. The simulated campaign targeted nearly 110,000 workforce members and included remedial training that reminds the workforce member of suspicious indicators when inspecting a potential phishing email.

Teleworking Security Tips

- ***Do*** use a secure wi-fi network
- ***Do*** log off or lock your devices
- ***Do not*** have business calls where anyone else can hear confidential information
- ***Do not*** click or download anything from an unknown account