WHOLE OF SOCIETY CYBERSECURITY

April 2024| Issue 2024:4

CYBERSECURITY IS EVERYONE'S RESPONSIBILITY

A whole-of-society approach to cybersecurity involves collaboration and coordination among all stakeholders to create a secure and resilient digital environment. It recognizes that it is essential for every individual to develop cyber skills to build this.

The Delaware Cyber Security Advisory Council, (DCSAC) is a statewide, cross-sector, multi-disciplinary group focused on mitigating the impact of cyber disruptions in the state and maintaining critical services for our citizens. Building resiliency requires government and industry to share cyber threat intelligence in real-time.

Cybersecurity attacks, including data breaches, corporate theft, and sabotage perpetrated by state and non-state actors present unique threats to Delaware residents, governments, businesses, and critical infrastructure. The 17 members of the Council include all branches of government, the military, education, public utilities, and the private sector. The Council's primary objective is to focus on sharing and analyzing cyber threat intelligence in a collaborative manner.

Private citizens have a role, too. Individuals must take basic cyber hygiene steps to prevent hackers from taking over their internet-connected devices and attacking corporate websites or critical infrastructure.

As a state employee you can contribute to our network's cybersecurity by completing the annual required training, staying current with the

CYBER-RISK IS MORE THAN JUST BUSINESS RISK

Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency (CISA), at a recent Congressional hearing on Chinese cyber operations, stated that there's a growing threat from and demand for a market for cyber vulnerabilities. More alarming was Easterly's assessment that "we've made it easy on" attackers through poor software design. To secure our systems and prevent a whole-of-society or whole-of-economy attack it will take a whole-of-society effort to secure cybersecurity market to create high-performing and secure technologies.

Our nation relies on connected technologies every hour of every day to enable essential services, from drinking water to electricity to financial systems. This dependence has deepened even further in recent years as many Americans now rely on connectivity for most aspects of their daily lives. Malicious cyber actors recognize our dependence on technology and constantly attempt to exploit this reliance for financial or strategic gain.

As CISA articulated in its Secure by Design initiative, vendors are the first step to creating secure and useable technologies. Taking security into account along with performance and features from day one of a product's development will help build a secure technology stack.

Federal agencies have launched a robust “whole-of-government” cybersecurity strategy focused on undermining adversaries, promoting network resiliency and sharing cyber threat information with infrastructure operators. However, a broader whole-of-society cybersecurity effort — involving state governments, corporations and ordinary citizens — is required to safeguard the critical infrastructure that keeps American society functioning.

The final piece of a whole-of-society approach to cybersecurity is both the most difficult and the most critical: integrating cybersecurity into the day-to-day lives of people. While CISA and the US government have placed much of the burden for secure development and secure decisions on companies, everyone must realize that the cybersecurity stakes go far beyond individual credit cards and bank accounts.

monthly "Restricted Intelligence" training and alerting your organizations' IT Security with questions or concerns about potential cyber intrusions. A simple step is to be familiar with the Phishing Alert Button, also known as PAB, and use it to flag any questionable emails.

Solomon Adote
Chief Security Officer

The doomsday scenario of a simultaneous power, water, and communications disruption brings these stakes into focus, and everyone must be willing to increase their cyber literacy and compliance to stop this scenario from unfolding. Just as we accept and comply with the incessant tones that remind us to buckle our seatbelts when driving, we must accept minor cybersecurity "nudges" like multifactor authentication for sensitive work and personal data.

READ MORE CYBERSECURITY NEWS at DIGIKNOW!

Delaware Department of Technology & Information publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links or want to print a PDF copy, go to:https://digiknow.dti.delaware.gov/news/index.shtml?dc=newsletters

Department of Technology and Information
Contact us at **esecurity@delaware.gov**