YOU ARE THE FIRST LINE OF DEFENSE

June 2021 | Issue 2021:5

CSO's Message

Greetings,

Did you know that a cyber-aware workforce not only protects our network and our citizen's data but it contributes to cost savings for state government? Delaware's bond and credit ratings can be affected positively or negatively based on the effectiveness of its cybersecurity controls. What do we mean by cybersecurity controls? These are the tools, processes, and services we invest in and deploy to safeguard our citizens' and organizations' data.

When the State reaches out to the finance and insurance markets for items like cyber insurance or bond hearings the markets require the state to attest to specific security controls like; Endpoint security, security awareness training, and testing of employees, amongst others. When applying to these markets, the State attests to having a world-leading Endpoint detection and response (EDR) solution to protect its computers. We also attest to our security awareness training and phishing testing. Our ability to prove their effectiveness can mean a significant cost savings for our state. If we were to experience a major security event without these programs, we could be denied a claim by our cyber insurance company, resulting in major impact to our budget.

These companies know that employees are often the first target of hackers in trying to breach an organization's defenses. It is easier to attack an

RIPPED FROM THE HEADLINES
Ransomware and Other Attacks

WE are entrusted with Delawareans' personal information all across state government. WE are the first defense against intrusions into the State and K-12 networks. That is why the annual cyber awareness training is so important for all of us. When you receive your training notification this summer, please give it high priority in your work schedule. Educating yourself makes our defenses stronger. Cyber criminals use your strong emotional reaction to force you to react right away, so they can exploit you. Don't let something create a false sense of urgency or fear that causes you or your employer to be a victim.

Ransomware data dumps can include the sensitive personal information of employees and customers, possibly leading to layoffs or even business shutdowns. As Javvad Malik, Security Awareness Advocate for KnowBe4, points out: "Whenever an organization is extorted via ransomware or other means, that money impacts actual individuals. Many people have lost their jobs and there have been organizations that have ceased to exist."

February 2021 - The city water treatment system in Oldsmar, Florida was breached. The attacker took over the control system and increased the levels of sodium hydroxide to deadly levels. The hacker gained access through TeamViewer, a commonly used application that gives workers access to all team members' computers. All the computers at the treatment system used the same password. Luckily, the employee with the hacked desktop noticed the intrusion and re-adjusted the chemicals to a safe level before anyone was physically affected.

April/May 2021 - A massive Facebook breach affecting over 500 million users' data was announced in April. May brought the Colonial Pipeline ransomware attack. The owners closed the line for five days, threatening the supply of gasoline for the entire East Coast. Ireland took all of its national health and social services systems offline for several days due to a ransomware attack.

The FBI reports that the Conti ransomware gang has hit at least 16 healthcare and emergency first responder networks in the U.S. Its victims' list includes law enforcement agencies, emergency medical services, 9-1-1 dispatch centers, and municipalities of various districts.

According to the FBI's Cyber Watch (CyWatch) researchers, Conti's operators infiltrate victim networks through phishing emails (malicious links or attachments) or stolen/cracked remote desktop protocol (RDP) credentials.

Their average recorded dwell time in the victim's network ranges between four days to three weeks. Moreover, when it comes to the ransom demands,

organization from the inside using social engineering and phishing than any other way. That is why they request this information from the state and why state leadership strongly requires your attention to security awareness training and phishing exercises.

there is no fixed number quoted by its operators. It widely varies depending on the targeted organization's size. However, the highest recorded bid of the Conti ransomware gang stands at $25 million.

These are just a few of the cyber attacks occurring increasingly more frequently. Ransomware attacks continue to hit public and private organizations across the country, including schools, hospitals, companies and local government sites, costing an estimated $3.6 billion in the U.S. in 2020.

READ MORE CYBERSECURITY NEWS at DIGIKNOW!

Delaware Department of Information & Technology 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.

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