School District of Cudahy

Cudahy, Wisconsin

Regular Board Meeting: August 26, 2024

Agenda Item: Cyber Security Update

Report Preparation: Brian Dasher and Rebecca Rentmeester

Background Information: The FBI notified us back in May that credentials belonging to an employee were discovered on the dark web. Their visit was primarily to inform us of this finding and gather information regarding potential security threats. At this time, we have no indication that our systems were or are compromised.

To ensure our systems remain secure, we have been actively working with Digicorp to thoroughly inspect our servers and firewall configurations. Digicorp has implemented a firewall rule to block inbound connection attempts from outside the United States. Additionally, Digicorp has implemented outbound traffic restrictions to Afghanistan, Bulgaria, the Czech Republic, Taiwan, and Russia as a precautionary measure.

Here are some other cybersecurity updates and measures we have implemented:

1) **Remote Server:** Public access has been restricted to only police IPs. We aim to finalize configurations for a tunnel interface VPN connection with the police department by the fall of 2024.
2) **CSDMain Network WiFi:** Password reset completed July 17th, 2024.
3) **Cybersecurity Services:**
    a) Endpoint Detection and Response (EDR):
        - **Purpose**: EDR solutions monitor and respond to advanced threats on endpoints (e.g., computers, servers, mobile devices).
        - **Key Features**: Anti-Ransomware capabilities protect against ransomware attacks by detecting and mitigating them before they can encrypt files. Application Control restricts unauthorized applications from running, enhancing security. Patch Management ensures all software and systems are updated with the latest security patches. Firewall integration enhances network security, and a Tune-up optimizes system performance.
        - **Provider**: Thirtyseven4, costing $2,292.50 annually.
    b) KnowBe4 Security Awareness Training:
        - **Purpose**: Educate all employees on recognizing and mitigating cybersecurity risks, including phishing attacks and tactics, beginning in the fall of 2024
        - **Importance**: Improves overall security by reducing the likelihood of successful cyber attacks from human error.

        - **Cost**: $14,491 annually.
    c) KnowBe4 Phisher Subscription:
        - **Purpose**: Provides ongoing simulation of phishing attacks to test and train employees' responses.
        - **Importance**: Helps assess and improve the organization's resilience to phishing threats, a common entry point for cyber attacks.
        - **Cost**: $8,051 for a three-year subscription.
    d) Penetration & Vulnerability Testing Externally:
        - **Purpose**: Test our five external public IP addresses to find vulnerabilities outside attackers could exploit. Find and rank vulnerabilities by severity.
        - **Importance:** We requested testing in May 2024 and were able to review the Qualys scan on our network, identify areas for improvement, and schedule regular testing. The previous testing was completed in 2021.
        - **Cost:** $445

These measures are crucial to maintaining our cybersecurity posture and protecting our organization from potential threats in the future.

Plan: Regular Cybersecurity Assessments, Enhanced Endpoint Protection, Employee Training and Awareness, Network Security Enhancements

Strategic Priority: Strengthening our organization's cybersecurity resilience.

Administrative Recommendation: Report only.

Action: N/A

Fiscal Note: N/A