NEW BRAUNFELS UTILITIES

MEMORANDUM

To: **NBU Audit Committee of the Board of Trustees**

From: **Greg Brown, Chief Technology and Security Officer**

Date: **November 30, 2023**

Subject: **Red Flag Report for 2023**

The Fair and Accurate Credit Transactions Act of 2003 (FACTA) required reasonable procedures to identify “Red Flags” defined by the Federal Trade Commission as "a pattern, practice, or specific activity that indicates the possible existence of identity theft." In response to the FACTA of 2003, New Braunfels Utilities (NBU) has adopted the Identity Theft Prevention Policy to mitigate potential threats via proactive measures and reporting. NBU implemented the Identity Theft Prevention Program to manage the following activities for “Red Flag” identification:

1. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the program;
2. Incorporate Red Flags already identified in existing NBU Policy into the program;
3. Describe and establish appropriate responses to any Red Flags as detected to prevent and mitigate identity theft; and
4. Update the Program periodically to assess changes in customer risk incidents, methods of risk identification or classification, supervisory oversight requirements, and training needs.

Incidents:

Customer Service stolen laptop:

On January 3, 2023 our customer service assistant manager had her laptop stolen. We proceeded to ask her probing questions in regards to the theft. This theft has a police report number T23000017 assigned to it. This laptop did not contain any customer files that could reveal any customer Personal Identification Information (PII) or Payment Card Industry (PCI) Data. This laptop was not logged into any active applications at the time of theft. The end user was encouraged to change her NBU password as well as any personal passwords to any accounts she may have accessed on said laptop.

Accomplishments

The Cybersecurity Team delivered on many planned goals in FY23. The accomplishments included the deployment of a modern endpoint management system with vulnerability scanning capabilities, the completion of two (2) program evaluations with recommended roadmaps defining a maturity path, a strategic plan that redesigns the program with a focus

on business interoperability and resiliency, and the acquisition of professional services to scale the program appropriately.

In March 2023, the cybersecurity team successfully deployed a modern endpoint management system (Taegis XDR). The robust cyber platform provides in-depth insights and awareness in the NBU technology infrastructure environment. The platform introduced a sophisticated vulnerability scanning function to identify critical vulnerabilities. This feature redefined the methods for remediation in the organization using a policy driven remediation table to generate baselines for future analysis.

The Cybersecurity Team completed two (2) program evaluations in FY23. The first was an automated process using the online tools from NBU's global technology partner, Gartner. The second evaluation was a more detailed process that consisted of on-site interviews with both technology and non-technology employees. The results from both evaluations included roadmaps defining a path to mature the program. These roadmaps were combined with internal gap assessment findings to create one centralized cybersecurity roadmap.

The Cybersecurity Team also developed a strategic plan that adopts the National Institute of Standards and Technology (NIST) framework. The framework is one of the most trusted methods for defining a set of guidelines to mitigate cybersecurity risks. The strategic plan aligns with the Technology Strategic Plan and the NBU Organizational Strategic Plan.

NBU has procured the professional services of a cybersecurity firm, iSphere, with a specialty in electric utilities. The firm has members on staff with national recognition in key areas that will be beneficial to strengthening our security posture. The firm's responsibility will include assistance with developing and deploying the existing roadmap, developing sustainable programs at the appropriate scale of the organization, refining reporting media, and Board level updates.

Per Texas House Bill 3834, our Cybersecurity and Learning & Development teams provided the following training required by the State of Texas:

Texas Cybersecurity Awareness Training 2023

- Topic Included:
  - Information Security Habits
  - Procedures that protect Information resources
  - Best practices for detecting, assessing, reporting, and addressing Information Security Risks

A total of 372 employees completed the training by July 18, 2023, a 100% completion rate.

NEW BRAUNFELS UTILITIES

MEMORANDUM

In Summary:

The existing Identity Theft, Red Flag, and Suspicious Activity detection methods as described in the NBU Identity Theft Prevention Policy continue to be reasonable, appropriate, and sufficient to mitigate risks to NBU and its customers.

Per Texas House Bill 3834, cybersecurity training and proof of compliance will be required annually. All NBU employees will be required to complete the training. The Cybersecurity and Learning & Development teams will continue to implement and deploy the training program.

Phishing Simulation Summary:

A phishing campaign is an attempt by threat actors to steal personal information that could compromise the integrity of the user's personal or corporate security. Phishing campaigns are executed via email where cybercriminals send fraudulent emails disguised as a trustworthy organization or reputable person. The goal of the phishing campaign is to obtain sensitive information that can be used to cripple an organization's ability to provide services to its customers.

In order to mitigate the potential damage resulting from a successful phishing campaign launched against NBU, the Cybersecurity Operations and Learning and Development teams work collaboratively to identify vulnerabilities in user awareness and provide follow-up training for those required. The program is a phishing simulation initiative whose goal is to train end users in the identification of social engineering tactics so they can make the right decision in the event of a real attack.

During the phishing campaign, the NBU average click rate for the past year is 4.75%, six percentage points lower than last year. The click rate is the percentage of end users that fail the simulation test. The Technology and Learning & Development teams will take remediation steps to lower the click rate by increasing training and continue phishing simulations for all end users. The goal of the phishing simulation initiative is to be below the utility industry click rate average of 5%.

NEW BRAUNFELS UTILITIES

MEMORANDUM

The information below details the phishing simulations for the past year.

Dates of Simulation	Subject of the Simulation	Results of the Simulation (Click Rate)
August 2022	HR: All Company Meeting Recap has been shared with you	9%
September 2022	IT@ has shared a printer with you	1%
October 2022	HR: Employee Data Review	2%
November 2022	Please review: Appropriate Halloween costumes	0%
December 2022	IT: Holiday travel with your work device	0%
January 2023	Inclement Weather Policy Update	18%
March 2023	Health and Safety Compliance Notice	4%
April 2023	HR: New requirements tracking Covid vaccinations	12%
May 2023	Celebrate National Chocolate Chip Day	1%
June 2023	IT: Updating Chrome Browser	1%
July 2023	June 10 - CEO Message	9%
August 2023	HRPaycheck	0%
September 2023	IT: ChatGPT Demand Survey	0%
October 2023	N/A	9%
November 2023	Reminder to activate your company LinkedIn Learning account	3%

MEMORANDUM

The chart below represents the Phish-failure Percentage. The click rate lowered after the increased phishing simulations and the establishment of the cyber warrior program.