City Council
Mayor Patrick Slayter
Vice Mayor Neysa Hinton
Una Glass
Sarah Glade Gurney
Diana Gardner Rich

City Manager
Larry McLaughlin
lmclaughlin@cityofsebastopol.org
Assistant City Manager/City Clerk, MMC
Mary Gourley
mgourley@cityofsebastopol.org

City of Sebastopol

Date: January 6, 2022

To: Larry McLaughlin – City Manager

From: Ana Kwong – Administrative Services Director

Subject: 2021 Cyber Incident

==========

The purpose of this memo is to address a public comment made by Mr. Kyle Falbo on January 4, 2022 City Council meeting. Mr. Falbo asked the following:

1. How was it possible for the breach to happen in the first place? How was it that the City staff email was accessed fraudulently to enact this crime?
2. What are the IT protocols of our City? What IT employee does our City have? How do we know this won't take place again as it did a month later with our Police Department?
3. How much has our insurance premium increased as a result of this?

The City Manager has provided updates and will continue to provide updates to the City Council and community regarding the fraudulent wire transfer that occurred in 2021. These funds were taken from the County of Sonoma that were held on behalf of the City of Sebastopol. City staff continues to work with the County, County and City Insurance Carriers and outside legal counsel for return of the missing funds. The City Manager will continue report out to the City Council and Community as this issue progresses through the claims process.

IT Needs and Supports:

The City of Sebastopol utilizes Microsoft 365 Office Systems City wide. In response to the recent cyber attack incident, the City of Sebastopol implemented MFA (Two Factor Authentication) in May of 2021. Completed a network wide password reset in June 2021 and recommends users change passwords at least semi-annually or as often as quarterly.

As the Council is aware, the City is conducting a City Wide Staffing Assessment to determine the personnel needs of this City, which includes those job functions that are being completed by outside consultants. Based on recent recruitments, it has been difficult to recruit personnel for not just City permanent staffing positions, but also has been difficult to recruit to fill our City volunteers positions. In some cases, consulting out for specialized services is a benefit, especially to a small City such as Sebastopol. This is currently the case with IT.

Finding and funding IT staff these days is no small task, regardless of whether we're a small, midsize or large organization. The positions needed in-house depend on the level of operations required. Organizations are relying more and more on a third-party partner to handle the monitoring, maintenance and security of its organizational infrastructure. Often times, a third-party partner can take on a heavy lifting for significantly less investment as the have the resources and personnel to address the multi-faceted aspects of IT security and allows the City to utilize the vast resources a firm has in place which a small City does not.

Most small and midsize organizations typically use a blend of internal and third-party providers to handle areas like desktop service support and security. With the increase in hacking, cyber attacks, identify theft, etc., it is getting more complex and detailed in the technical world, therefore, many smaller cities often conduct Request for Proposals (RFP) from outside consultants to obtain the more specialized skills needed to ensure the safety and security of IT. Larger agencies that have funding available for personnel costs such as Salary, Benefits, CalPERS liabilities, Overtime, etc., can justify hiring specialists on a full-time basis. The City of Sebastopol is not one of those larger organizations and has always outsourced IT support, maintenance and security. In 2017, Marin IT was selected as the City's IT consultant to manage the City's network. Their responsibilities for support allowed for the City to continue daily operations including but not limited to:

- Onsite support for Police Department.
    - IT staff is on site once every other week to conduct system maintenance, addresses any staffing issues, and conduct updates to system
- Onsite support for all other City Departments
    - IT staff is on site every week to conduct system maintenance, addresses any staffing issues, and conduct updates to system
- Desktop virus software updates / maintenance
    - IT has set computers to deploy updates automatically
    - Implemented web root 24/7 monitoring for all desktop devices
- Maintenance of desktop OS patches
    - IT conducts the patches as needed
- Local user account maintenance
    - IT conducts users issues weekly or special requests are handled as they are received
- Hardware maintenance
    - IT is responsible for maintenance of server; however City is responsible for purchase of equipment
- Mail client support
    - IT is responsible for creating/deleting Mail accounts
    - Special requests are handled as they are received
- VPN client support
    - IT provides security set up/protocols for staff that utilizes VPN
- Firewall to defend from cyber attacks and firewall
    - IT conducts maintenance / updates on Firewalls
    - Keeps abreast on awareness of cyber attacks and maintains system to ensure security
- Router & Switch
    - IT configures and maintains routers/switch
    - Conducts security updates
- Assistance with installation of new equipment / applications
    - IT installs all programs required by the City of Sebastopol
    - IT updates programs as needed
- Monitor local backup systems
    - IT reviews and conducts corrective measures
- Local windows domain
    - IT conducts maintenance to include local name resolution, server troubleshooting, and assistance of local security policies as needed
- Availability to assist with design and integration of new applications into local network

    - Example scheduling software, credit card processing
- Desktop /Server/LAN and WAN Misc. troubleshooting and resolution

Training for City Employees:

- Encouraging Email Vigilance - Remind users to be vigilant of suspicious e-mails from unknown sources and to not open file attachments or click on links; and reminders to look for suspicious requests, attachments, links and forged sender identities (phishing email)
- Email encryption when sending private information
- Providing access to cybersecurity awareness training through our insurance partners
- Avoiding Personal Devices For Work
- Communication to employees to not use auto-save for passwords
- Utilization of virtual private network, or VPN. A VPN encrypts everything that passes through, improving cybersecurity. This protocol is in place for our staff, and this policy ensures that all employees access via an encrypted tunnel
- Subscription to Proofpoint – this is a measure put in place from the beginning to prevent spam from getting into your mailbox

The City is working with CIRA and Marin IT to create City Policy on IT Security of City Computers and Training for City Employees.