Y2K SECURITY RISK ASSESSMENT

DEVELOPED BY TEAM Y2K: BOBBY BLOUNT, DONALD BOWLER, ANNA FREDRICKSON, JESSE GARZA, JOE LOUIE CORPORAL, ETHAN RUPP, MARCUS LOPEZ, BEZALEEL SAINZ.

Executive Summary

This is a cybersecurity assessment of Gemini Ink. The organization has contacted Team Y2K to assess weaknesses and providing recommendations for their operations. The organization's operations and systems include a team of employees, laptops, handheld electronic devices, microphones, and speakers. Based on the NISTIR 7621 Rev 1 Framework, we constructed a security guideline that provides detailed instruction for the organization to implement.

Team Y2k has contacted the Marketing Director Anisa Onofre and Information Technology support TJ Mcbride from Alamo PC & Mac for interviews, audits, and asked additional questions to further expound on this assessment. A checklist was implemented to provide a basis for what procedures and operations were in place for the organization along with a comment section that provided a detailed analysis of what the organization provided. Our findings are based on this checklist and the observations we have made from it. At the end of our assessment, we provide recommendations along with a checklist for future reference to maintain optimal practices and ensure a secure future for the organization.

We express our gratitude to Gemini Ink for granting us this opportunity, and we extend our appreciation to the Marketing Director, Anisa Onofre, for her complete cooperation during this assessment. The information shared by Ms. Onofre has been instrumental in identifying several vulnerabilities that may have gone unnoticed otherwise. We would also like to acknowledge the Information Technology support provided by TJ Mcbride, which contributed significantly to the success of this assessment. We look forward to the opportunity to continue our collaboration with Gemini Ink in the future.

Table of Contents

1 Introduction

1.1 Background

Gemini Ink has hired Team Y2K security consulting to establish Information Technology operation standards and provide security recommendations. Gemini Ink wants to limit access to confidential data and establish a data retention policy. Recording classes have become overwhelming, and they are considering a backup solution like cold storage. Team Y2K will help ensure data security and organization for Gemini Ink.

Team Y2K is meant to provide a baseline standard during this assessment to create a standard that will help avoid any future cybersecurity threats for the organization.

1.2 Scope

The in-scope for this assessment included virtual meetings with Marketing Director Anisa Onofre, where we discussed the company's operations and the security audit checklist. Team Y2K was provided with details such as the number of employees and the technology used in their processes. There were no standards for in-person meetings, however further contact was sent through email for any additional questions. All contact and questions were directed to Ms. Onofre, who was very cooperative and provided us with all necessary information. Gemini Ink's IT support specialist TJ Mcbride also gave us IT guidelines that were crucial to the success of this assessment.

1.3 Report Organization

The report is organized as follows: Section 2 provides an overview of the facilities, systems, and processes used by Gemini Ink. Sections 3 and 4 describe the methodology and activities undertaken by the team. Section 5 presents the assessment results, while Section 6 contains conclusions and recommendations for future actions. Additional information related to the assessment can be found in the appendices.

2 System Overview

The systems being evaluated are those outlined in the audit checklist provided to us by Gemini Ink. In addition, we have taken note of findings and comments gathered during interviews that provide further insights into these systems, which were not covered in the checklist. A thorough understanding of these systems is critical in order to provide the best possible security options for Gemini Ink. The level of detail provided enables us to conduct a comprehensive assessment and develop appropriate security measures.

2.1 Laptops

There are 7 laptops in use at the premises over at Gemini Ink. Any software for fulfilling job responsibilities is installed by employees when necessary. Any updates or software installation processes are done during the time needed or by the IT support specialist.

Key items:

Laptops are kept at the organization. They can connect to any network and install third party software. Employees have separate accounts when storing files and can access any of the laptops through their accounts from any laptops. Laptops are not stored in a secure location and are not inventoried. Laptops have no logs based on who has accessed a specific laptop.

2.2 Square

The square financial device is used at Gemini Ink for transactions processing credit card and debit cards. Any necessary software updates or installations are done by Square automatically. The square device is also kept at the facility.

Key items:

Square maintains logs of all transactions and access, including the date, time, and user information. Any suspicious activity or attempts at unauthorized access was immediately flagged and reported to the appropriate personnel for investigation.

2.3 Non-Profit Google Account

Gemini Ink uses a non-profit Google account, which is accessed by multiple users, including past clients and interns. Alexandra and TJ are the designated administrators of this account. All users work on the same account, which presents a potential single point of failure.

Key Items:

In the event of a compromise, it is unclear if the organization has a contingency plan in place to continue operations. The Google drive is cluttered with data, and implementing access control on each folder is time-consuming and challenging due to the sheer volume of data. Gemini Ink is concerned about the confidentiality of the data stored in the drive and wants to ensure that only authorized personnel have access to it.

3 Assessment Methodology

To establish a secure environment for conducting business at Gemini Ink, we have curated a cybersecurity model mostly from the NISTIR 7621 Rev 1 Framework, which is tailored towards small businesses. To simplify the framework, we have selected specific checks that are most important for Gemini Ink. This section will provide strategies and common practices for addressing security concerns and other issues typically found in smaller organizations. A checklist has also been included at the end of this report for clarity and importance.

3.1 Risk Management:

Risk management involves identifying and prioritizing the information that a business stores and uses, as not all information requires the same level of protection (2.2 NISTIR 7621 Rev 1). Personal information may be valued higher and legal costs lower, for instance. To safeguard this information, we have identified key checks based on the five categories of the framework: **Identify, Protect, Detect, Respond, and Recover.** This approach allows for a more targeted and effective security strategy.

3.1.1 Identify:

Identify and control who has access to your business information. NISTIR 7621 Rev 1 pg. 16

To limit access to confidential data and ensure its security, Gemini Ink needs to identify and control who has access to their business information. This task should be easier to manage since Gemini Ink has a smaller number of employees. The first step is to determine who has or should have access to the company's information and technology, and whether a key, administrative privilege, or password is required. Gemini Ink must be aware of anyone who has access to their business, including cleaning crews and maintenance personnel, and not allow unknown or unauthorized persons to have physical access to any of their business computers. Computer or network repair personnel should not work on systems or devices unsupervised. It's important to ensure that no unrecognized person can enter the office space without being questioned by an employee, as a criminal can easily steal any private or sensitive information on an unlocked machine if they gain physical access.

Conduct background checks. NISTIR 7621 Rev 1 pg. 16

It's recommended that Gemini Ink conduct full background checks on all employees to ensure their standing and history with the company. This includes doing a full, nationwide, criminal background check, sexual offender check, and if possible, a credit check on all prospective employees, especially if they will be handling business funds.

Require Individual user accounts for each employee. NISTIR 7621 Rev 1 pg.17

Individual user accounts for each employee should also be required. Gemini Ink should set up a separate account for each user (including any contractors needing access) and require strong, unique passwords for each account. Even changing their passwords within a specific time period of their choosing. Without individual accounts for each user, it may be difficult to investigate data loss or unauthorized data manipulation. All employees should use computer accounts without administrative privileges to perform typical work functions to hinder any attempt-intentional or not-to install unauthorized software. Gemini

Ink may also consider using a guest account with minimal privileges if needed for their business.

3.1.2 Protect:

Limit employee access to data and information. *NISTIR 7621 Rev 1 pg. 18*

It is essential to limit the access of employees to the Google Drive account, laptops, and Square financial devices of a business. Employees should only be granted access to the specific information and systems required for their job. Allowing an individual to have access to all the business's information and systems, including financial, personnel, inventory, and manufacturing, increases the risk of insider threats. Insider threats are one of the main sources of security incidents, and they can cause intentional or unintentional harm to the business. It is vital to ensure that no single individual can initiate and approve transactions, even executives and senior managers.

When an employee leaves the business, the company should revoke their access to the Google Drive account, laptops, and Square financial devices. This involves collecting their business ID, deleting their account and username from all systems, changing any group passwords or combination locks they may have known, and collecting any keys they were given. This precaution will prevent any unauthorized access by former employees and safeguard the business's sensitive information.

Patch your operating systems and applications. *NISTIR 7621 Rev 1 pg. 18*

Installing any software application, including operating systems, firmware, or plugins, on a system can potentially create a pathway for cyberattacks. To minimize this risk, businesses should only install necessary applications and regularly update and patch them. Software vendors often release patches and updates to their products to address security concerns and improve functionality. It is crucial to know how to update and patch all software on each device, including Google Drive accounts, laptops, and financial devices.

When purchasing new computers or installing new software, is it essential to check for updates immediately? Only current and vendor-supported versions of software should be installed, as vendors are not obligated to provide security updates for unsupported products.

To ensure that all software is up-to-date, businesses may find it helpful to assign a specific day each month to check for patches. There are tools available that can scan systems and alert users when an update is available for a particular application. However, it is important to make sure that these tools scan for updates for every application in use. Another way to check for updates is to go directly to the original manufacturers of installed applications. By following these practices, businesses can minimize the risk of cyberattacks and protect sensitive information.

Install and activate software and hardware firewalls on all your business networks *NISTIR 7621 Rev 1 pg. 18*

To prevent unwanted Traffic and potential cyberattacks, businesses should install and operate hardware and software firewalls. A hardware firewall should be installed between the internal network and the internet. Consider changing administrative login credentials and enable logging to aid in investigation. Install a software firewall on each computer system used and ensure that it is updated regularly. Use updated and vendor-supported versions of firewalls. It is necessary to have firewalls even when using cloud services or VPN. for employees working from home, ensure they have hardware and software firewalls installed and updated. Consider installing an Intrusion Detection/Prevention System for increased protection.

Dispose of old computers and media safely. *NISTIR 7621 Rev 1 pg. 21*

When disposing of old computers, wipe the hard drive(s) electronically, physically remove them, and have them destroyed. Install remote-wiping applications on mobile devices to erase all information in case of loss or theft. Delete any sensitive data from old media (CDs, USB drives, Google Drive, etc.) before shredding or having it destroyed. Use a crosscut shredder to destroy paper containing sensitive information. Consider incinerating very sensitive paper and media.

Train Employees. NISTIR 7621 Rev 1 pg. 22

Train employees immediately and at last annually thereafter about information security policies. Ensure they understand the penalties for not following policies and have them sign a paper stating they will comply. Train them on appropriate use of company computers and mobile devices, how to treat customer information, and what to do in case of an emergency or security incident. Obtain training from various organizations such as SBDC or SCORE Chapter. Continually reinforce training in everyday conversations, meetings, or newsletters to develop a culture of security in employees and the business.

3.1.3 Detect:

Install and update anti-virus, -spyware, and other -malware programs. NISTIR 7621 Rev 1 pg. 23

Malware is harmful software that can steal or damage information. Install and update anti-virus and anti-spyware software on every business device. Schedule automatic checks and scans for updates and malware at different times. Obtain copies of anti-malware software for employee devices or require them to have it. Use two different anti-virus solutions from different vendors for improved detection. Do not exclusively rely on firewalls or other systems to protect the network. Malware can record your actions or send sensitive information to cybercriminals. It is important to regularly update and scan for malware to prevent data breaches. Consider real-time scans for increased security. Ensure anti-malware software is used on personal devices used for work. Malware can use up computing resources and cause harm to devices.

Maintain and monitor logs. NISTIR 7621 Rev 1 pg. 23

Hardware and software used for protection and detection, like firewalls and anti-virus software, should be set to log activity. Ensure this feature is enabled and backup and store logs for at least a year. Consider having an IT support specialist review the logs for unusual trends. Logs can identify suspicious activity and be valuable in investigations. Keep a log of people who enter or leave the facility as an additional security measure. Some logs may need to be stored for a minimum of six years. Unusual trends in logs may indicate a more serious problem or the need for strong protection in a specific area.

3.1.4 Respond:

Develop a plan for disasters and information security incidents. NISTIR 7621 Rev 1 pg. 23

Develop a plan for immediate action in case of emergencies, such as a fire, medical emergency, burglary, or natural disaster, for your organization with its associated electronic devices. Roles and responsibilities should be assigned, including who will make recovery decisions and be in contact with law enforcement. Determine what to do with information and systems during an incident, like shutting down computers and physically removing important documents. Create a list of relevant contacts, including senior executives, emergency personnel, cybersecurity and legal professionals, service, and insurance providers, and be aware of notification laws in your area. Include procedures for each job role during an emergency. Consider developing a procedure document that outlines specific actions employees should take. Also, define what activities constitute an information security incident, like website downtime or evidence of information being stolen. Be aware of when to notify authorities, such as your local police department or FBI office.

3.1.5 Recover:

Make full backups of important business data/information. NISTIR 7621 Rev 1 pg. 23

Create backups of all data on each laptop and mobile device used by the organization, at least once a month, and store them securely away from the office location. Backup only the data, not the software applications themselves. Removable media like an external USB hard drive or cloud storage can be used for backup. Select a cloud service provider carefully and encrypt all data prior to storing it in the cloud. Use a separate folder for each computer when connecting to the external disk for backups. Perform the backup shortly after running a full virus scan. Keep a copy of the encryption password or key in a secure location. Backup all data, including word processing documents, electronic spreadsheets, databases, financial and human resource files, system logs, and other business information. Without data backups, the organization may have to recreate business information manually.

Make improvements to processes / procedures/ technologies. NISTIR 7621 Rev 1 pg. 23

You may want to consider conducting training or table-top exercises which simulate or run-through a major event scenario in order to identify potential weaknesses in your processes, procedures, technology, or personnel readiness. Make corrections as needed.

4 Assessment Activities

This section covers the activities performed by the assessment team. The observations and findings made from these activities are discussed in Section 5.

4.1 Gemini Ink Audit Review

The Y2K Consulting team has reviewed the operations of Gemini Ink, provided by the marketing director. This review contains information based on the technology used, the workspace the organization precedes in, and the number of employees they currently hire.

4.2 In-person Interviews

On April 5th, 2023, the team met with Marketing Director Anisa Onofre to discuss the Gemini Ink facilities and goals to identify what cybersecurity policies and vulnerabilities they have in place.

On April 21st, 2023, the team met with the Marketing Director once again for the audit procedures for their daily operations and detailed their security policies in place. Additional questions were asked through email to establish further detail that aids in providing recommendations. Through these discussions, we were able to pinpoint several areas that raised concerns and numerous areas that aligned with best practice guidelines.

5 Assessment Results and Recommendations

This section presents the outcomes from the analysis of the overview document and the interviews with Gemini Ink's Marketing Director, Anisa Monroe. The section encompasses weaknesses, strengths, and observations. Weaknesses refer to findings that may pose a vulnerability or offer an opportunity for an attacker. The priority level for each weakness is indicated as HIGH, MODERATE, or LOW. Strengths highlight areas where Gemini Ink's practices are commendable. Observations cover findings that are not necessarily weaknesses or strengths but require some reconsideration or fall outside the scope of analysis.

5.1 Strengths

Backups:

Necessary backups are done on the iMac for critical data and are done regularly, having a physical location or cloud based service to do the backup. Gemini Ink makes sure to make improvements where it is needed over time, in order to execute backups efficiently and properly.

Physical Security:

Temporary badges are distributed to Gemini Ink volunteers during large events. Gemini Ink has a designated area for shredding physical documents.

Software Updates:

Confirmed by the IT support specialist and the Marketing Director, anti-virus and general software is updated and used on a regular basis in the organization.

Personnel Security:

Staff have unique login credentials and separate accounts with multi-factor authentication, ensuring secure access. Staff are knowledgeable of how to respond, handle, and detect malicious emails or websites. The access to company information is also revoked when they leave the business, ensuring corporate data stays within the organization. All staff and volunteers have access to policy handbooks for training. In the event of a security breach or cyber-attack, employees know to contact their Information Technology Specialist, to minimize data leakage. Employees are also trained and aware of which areas must be sealed off in the event of an emergency.

5.2 Weaknesses

(High) No Procedures for Compromised Passwords

Justification:

Having procedures for compromised passwords is needed for maintaining the security and integrity of an organization's data and systems. Passwords are a common authentication method used to protect access to sensitive data and systems of an organization. If a password is compromised, it can lead to unauthorized access, data breaches, and in some situations access to any financial information the organization or individual has. While NISTIR 7621 Rev 1 does not have any direct sections dedicated to compromised passwords, a recommended source of documentation is the NIST Special Publication 800-63B under section 6.2 *Lost, Theft, Damage, and Unauthorized Duplication*. The publication provides guidelines for digital identity proofing and authentication, including recommendations for password policies and procedures.

Recommendation:

Team Y2k recommends developing a procedure on compromised passwords centered around resetting passwords, disabling accounts when a cybersecurity event has been initiated, and investigating the source of where the compromise took place. Additionally, the organization can do a password audit where they can identify weak passwords and password reuse. Password audits can include reviewing password policies, identifying patterns in password use, and testing password strength. Gemini Ink can implement strong password usage by creating a password that is at least eight characters long, that contains at least one uppercase letter, at least one lowercase letter, at least one number, and at least one symbol.

(Moderate) No periods of scheduling password changes

Justification:

Passwords that do not change for long periods of time allow hackers time to crack them and may be shared and become common knowledge to an individual user's coworkers. So according to NISTIR 7621 Rev 1 *4 Working Safely and Securely*, passwords should be changed at least every three months, as passwords to devices and applications that deal with business information should not be re-used.

Recommendation:

As stated by the NIST framework, a password change every three months is considered a good routine. Using a password management system would be a good option, as remembering a different number of passwords is difficult. These systems securely place all passwords into one place. Carefully compare password management solutions before purchasing. Bitwarden is an example of a popular password management solution that can be free of charge with creating a personal account and alerts you if there has been a data breach. While it is not widely recommended, staff can keep physical documentation on paper of their passwords as long as the physical documentation is securely stored away from unauthorized persons. Having physical documentation of passwords can be safe because cyber-attacks cannot use password information to infiltrate company accounts unless they physically enter the facility.

(Moderate) Electronic Devices Not Inventoried

Justification:

While NISTIR 7621 Rev 1 provides guidelines for inventorying devices in an organization's facility, it is not always feasible to include all electronic devices such as tablets, laptops, and Square financial devices. These devices may be owned by employees or contractors and used for personal or business purposes, making it difficult to track and inventory them.

However, just because these devices are not included in the inventory does not mean they are exempt from cybersecurity measures. In fact, these devices can be just as vulnerable to cyber-attacks as any other device in the facility. Therefore, it is important to ensure that appropriate cybersecurity measures are in place for these devices.

Additionally, the use of Square financial devices for payment processing can result in financial losses for the organization in the event of a data breach. These devices can be targeted by cybercriminals seeking to steal credit card information, which can result in costly chargebacks and damage to the organization's reputation.

Recommendation:

To ensure electronic devices such as tablets, laptops, and Square financial devices are properly secured, organizations can use NISTIR 7621 Rev 1 as a basis for cybersecurity recommendations, using NISTIR 7621 Rev 1 2.2 *Managing Your Risk* as reference. Monitor devices for unauthorized access or suspicious activity and as well, under specific time periods, inventory the total amount of devices used in the organization, also inventorying the software and hardware used in daily operations to ensure secure systems. Gemini Ink can implement this plan through numbering all devices and developing a simple sign in/sign out sheet that documents the time a device was taken out, the time a device was returned, the name of the person signing the device out, and the date that the device is being used.

(Moderate) No Monitoring Logs for Devices Accessed

Justification:

Creating a monitoring log system to authenticate who is using what device is essential for maintaining the security and integrity of an organization's data and systems. The system can help prevent unauthorized access to sensitive data, reduce the risk of data breaches, and ensure accountability for device usage.

Devices such as tablets, laptops, and Square financial devices not logged can still pose a significant risk to an organization's cybersecurity. If these devices are not properly managed and authenticated, they can be easily lost or stolen, leading to potential data breaches or financial fraud. Additionally, without proper authentication measures in place, it can be challenging to determine who accessed a particular device or data, making it difficult to track down security incidents and potential threats.

A device checkout system can help address these risks by ensuring that only authorized users have access to devices and data. By requiring authentication before allowing access, the system can help prevent unauthorized access attempts and limit the potential impact of a security breach.

Therefore, creating a device checkout system is a crucial cybersecurity measure for organizations that want to protect their data and systems from potential threats and ensure accountability for device usage.

Recommendation:

There is information for monitoring logs in NISTIR 7621 Rev 1 3.3 *Detect*, the recommendation for monitoring logs is to develop a device inventory, implement a device checkout system, and then enforce device usage policies where usage is used to identify potential security incidents or threats. Monitoring can include reviewing logs, identifying anomalous activity patterns, and detecting unauthorized access.

(Moderate) Background checks for employees and Visitors

Justification:

Background checks for employees and visitors are essential for maintaining the security and integrity of an organization's data and systems. Specified in NISTIR 7621 Rev 1 3 *Safeguarding Your Information*, background checks can help identify potential risks and threats, such as criminal history or other indicators of malicious intent. By identifying potential risks and threats, organizations can mitigate the risk of stolen data, equipment, or compromised operations.

Therefore, conducting background checks for employees and visitors is a crucial cybersecurity measure for organizations that want to maintain personnel security and protect their data and systems from potential threats.

Recommendation:

Team Y2k recommendation is to conduct background checks for new employees and any necessary background checks for visitors where sensitive data will be exchanged. Assign role on the faculty staff to handle this assignment to mitigate duties. Background checks should include social security verification, evidence of a criminal record, drug testing, credit check, employment history, and motor vehicle record if they are required to drive in their job title. Whichever employee is picked to conduct the background checks, must make the candidate aware that they are conducting a background check and must make sure that they are following their state regulations for what information is allowed to check on Texas' public safety website. Background check websites can be utilized but typically require a payment subscription for the reports. Some of the most reputable background check software includes BeenVerified, TruthFinder, and Intelius.

(Low) Badges for Staff Members

Justification:

Having badges for staff members is essential for maintaining physical security and access control in an organization. Badges can help identify authorized personnel and restrict access to sensitive areas, equipment, and data. By ensuring that only authorized personnel have access to these areas, organizations can prevent unauthorized access, theft, and data breaches.

Physical security is a critical component of a cybersecurity strategy, as it helps protect against insider threats and unauthorized access to sensitive data. You can find more information on Physical Security under NISTIR 7621 Rev 1 *Background: What is Information Security and Cybersecurity?*

Recommendation:

Team Y2K recommends issuing badges to authorized personnel and developing an access control policy that outlines the requirements for access to sensitive areas, equipment, and data. The policy should define who is authorized to access these areas under what circumstances. Implementing physical security controls such as locks, security cameras, or alarms would additionally aid access control. Gemini Ink can implement badges for authorized personnel by purchasing plastic name tag holders and lanyards. These plastic name tag holders can be found in sets for an affordable price on Amazon. The name tag portion of the badge can be created for free on a website called VistaCreate. VistaCreate requires all users to create an account, however, building personalized cards of all shapes and sizes is free to download and print. Gemini Ink can design and create their own badge cards, handwriting their names on them and then insert the cards into the plastic name tags.

5.2 Observations

-employees and visitors should carry identification when inside

-IT works remotely

-access to building should have a log system to identify who has been there

Employees decide what cyber security awareness training they do.

Some security awareness training is better than no training at all. However, this should not also be one and done training, it should be at least done annually to keep employees vigilant and prepared for cyber-attacks.

Employees and visitors should carry identification when inside the facilities.

Employees and visitors should carry identification to verify their identity and to track visitors. Identification can be helpful in case of an incident, such as a fire or medical emergency, to identify victims and witnesses quickly and accurately.

Access to the building should have a log system to identify who has been there.

A log system can help to ensure that only authorized people are entering and leaving the facility. If an incident occurs, a log system can help investigators to identify who was present at the time of the incident.

6 Conclusions and Follow-on Activities

6.1 Conclusion

The cybersecurity assessment of Gemini Ink identified several strengths and weaknesses. The organization has a variety of strong cybersecurity practices in place, including regular backups, software updates, and multi-factor authentication for staff. However, there are also a few areas where Gemini Ink could improve its cybersecurity posture, including inventorying electronic devices, implementing a device checkout system, monitoring device logs, conducting background checks for employees and visitors, and developing procedures for compromised passwords. Although we were not able to assess every single possible vulnerability that an attacker might target, we believe that the recommendations provided in this report will help Gemini Ink improve their cybersecurity posture and awareness of the threat that a cyber-attack poses to the organization.

6.2 Follow-on Activities

Based on the findings of Y2K Security Risk Assessment, Gemini Ink may also implement the following follow-on activities:

- Update Inventory all electronic devices, including tablets, laptops, and Square financial devices whenever new devices are added and old devices removed.
- Implement a policy that requires all devices that are returned to the organization to be formatted before they are reused.
- Secure network equipment. Keep Wi-Fi routers and network switches out of reach or behind a locked cabinet. Disable unused Ethernet ports. This will prevent an attacker from connecting to your network without a password.

- Lock computers and workstations when unattended. Employees should lock their computer or workstation when leaving their desk. This will help to prevent unauthorized access to sensitive data.
- Remove any user in the organization's Google account who no longer need access.

Implementing a security awareness training program for employees and interns as part of the onboarding process.

By implementing these follow-on activities, Gemini Ink can further improve its cybersecurity posture and reduce its risk of a data breach or other security incident.

7 Y2K Cybersecurity Risk Assessment

Answers obtained from Anisa Onofre, Gemini Ink's Marketing Director, on April 21st.

CYBERSECURITY RISK ASSESSMENT

THE FOLLOWING ARE QUESTIONS BASED OFF OF THE NIST 7621 REVISION 1 CYBERSECURITY FRAMEWORK FOR SMALL BUSINESS INFORMATION SECURITY.

INTERVIEW: ANISA ONOFRE, GEMINI INK'S MARKETING DIRECTOR 4/21 10AM

IDENTIFICATION PROCEDURES

	SELECT ONE: YES/NO	COMMENTS
Are devices and systems within the organization inventoried?	☐ YES ☒ NO	Computers, tablets, recording devices, mics, speakers are the devices that they own… They tried to inventory them in the past but did not stick with it.
Do all staff members have badges that are all authorized?	☐ YES ☒ NO	
Do you provide temporary badges for visitors?	☒ YES ☐ NO	Yes, only for large events for their volunteers, they do not have badges for their employees for access to the building
Do you have a procedure for obtaining/discarding badges for staff members upon termination?	☐ YES ☒ NO	They ask for people to turn them in but the rule is not always followed, some take them home
Do staff members have to update their photo IDs over a certain amount of time?	☐ YES ☒ NO	
Do you conduct background checks for employees and visitors?	☐ YES ☒ NO	Only for those in the partner class programs.
Do you check the credentials of all visitors?	☐ YES ☒ NO	

Do visitors have to carry any form of identification with them through the facilities?	☐ YES ☒ NO	
Are staff members' and visitors' identification badges/IDs easily differentiated?	☐ YES ☒ NO	
Do visitors have access to company computers?	☐ YES ☒ NO	Interns have access to their office laptops
Do you have a policy handbook for staff members to access?	☒ YES ☐ NO	

PROTECTION OF PERSONAL & PHYSICAL SECURITY

	SELECT ONE: YES/NO	COMMENTS
Do you provide staff training from certified Information Technology (IT) experts on cybersecurity?	☐ YES ☒ NO	
Do you provide training regularly?	☐ YES ☒ NO	Offered regularly, but they decide what training they do for themselves. Watching videos online etc.
Does your staff know how to respond to scams or malicious emails/websites?	☒ YES ☐ NO	
Are your employees trained to point out scams or malicious emails/websites to your Information Technology Specialist (IT)?	☐ YES ☒ NO	Their just take care of them on their own.
Are your employees trained to use secure passwords?	☐ YES ☒ NO	Use their own passwords
Do you have a procedure in regard to compromised passwords?	☐ YES ☒ NO	
Do you conduct regular audits of security requirements and plans?	☐ YES ☐ NO IDK	
Do you have a firewall installed on all company devices?	☐ YES ☐ NO IDK	

Do you update your firewall and patch all software downloaded on company devices?	☐ YES ☐ NO IDK	
Do you update all physical hardware to the last firmware or replace them over time? (Routers, laptops, servers, SSDs, etc.)	☐ YES ☐ NO IDK	
Are there any monitoring or back logs of activities of the firewall?	☐ YES ☐ NO IDK	
Do you keep inventory of all authorized devices?	☐ YES ☐ NO IDK	
Do you regularly test all systems for vulnerabilities?	☐ YES ☐ NO IDK	
Is all confidential data encrypted?	☐ YES ☐ NO IDK	
Do you have places for shredding physical documents?	☒ YES ☐ NO	
Do you have places and a procedure for disposal of electronic media?	☐ YES ☒ NO	
Do your staff members have any limitations on altering or accessing media based on roles in the organization?	☐ YES ☒ NO	
Does each staff member have unique login credentials?	☒ YES ☐ NO	
Does each staff member have separate accounts used for the various software and hardware?	☒ YES ☐ NO	
Does your organization use surge protectors to protect your electronic devices?	☐ YES ☐ NO IDK	
When a staff member leaves the business, are they revoked access to company files?	☒ YES ☐ NO	
Have you secured your wireless access point and networks?	☐ YES ☐ NO IDK	

Do your staff members' accounts utilize multi-factor authentication?	☒ YES ☐ NO	Sometimes, few accounts that require an email/text code to be sent to them to input

DETECT NATURAL & CYBER THREATS

	SELECT ONE: YES/NO	COMMENTS
Do you keep a detailed log that shows who accessed what authorized devices or applications at specific times?	☐ YES ☒ NO	
Are these logs backup and stored remotely in case of an emergency?	☐ YES ☒ NO	
Do your employees know where and what to do with sensitive data in the event of an attack?	☐ YES ☒ NO	
Do your employees know who to contact if an insider employee has launched a cyber-attack?	☒ YES ☐ NO	IT person does
Do you have anti-virus or malware software(s) on your systems?	☐ YES ☐ NO IDK	
Do you have a procedure for monitoring weather in times of possible severity?	☐ YES ☒ NO	

RESPOND

	SELECT ONE: YES/NO	COMMENTS
Do key employees know how to seal off designated areas in your facility if necessary?	☒ YES ☐ NO	
Do you have emergency evacuation plans for employees?	☐ YES ☒ NO	
Have you regularly tested this emergency evacuation plan with your staff members?	☐ YES ☒ NO	

Are these emergency plans easily accessible for staff members in the printed forms?	☐ YES ☒ NO	
Do you have emergency shelter in place kits for employees if they cannot leave your facility?	☐ YES ☒ NO	

BUSINESS CONTINUITY & DISASTER RECOVERY

	SELECT ONE: YES/NO	COMMENTS
Do you have the technology to create backups of critical data?	☒ YES ☐ NO	Backups on iMac at work, doesn't know if everyone has one or implements it
Does your company backup critical data regularly?	☒ YES ☐ NO	
Do you run tests regularly to ensure that the backups are working and recoverable?	☐ YES ☐ NO IDK	
Are the backups stored in a physical hard drive or on the Cloud?	☒ YES ☐ NO	
Are backups and encryption keys kept separate from other sources of data?	☐ YES ☐ NO IDK	
Does your company implement a procedure for recovery when a disaster strikes?	☐ YES ☒ NO	
Does your company update the recovery procedure regularly?	☐ YES ☐ NO IDK	
Does your backup plan involve a method for accessing encryption keys in an emergency?	☐ YES ☒ NO	
Does your company have a form of cyber insurance?	☐ YES ☐ NO IDK	
Are you making adjustments and improvements to these processes over time?	☒ YES ☐ NO	

OUR TEAM HAS THE KNOWLEDGE AND SKILLS TO KEEP YOUR BUSINESS SAFE.

FOR ANY INQUIRIES, PLEASE CONTACT OUR TEAM LEAD, BOBBY BLOUNT, VIA EMAIL AT
bobby.blount@secure.gcomet.net

DEVELOPED BY TEAM Y2K: BOBBY BLOUNT, DONALD BOWLER, ANNA FREDRICKSON, JESSE GARZA, JOE LOUIE CORPORAL, ETHAN RUPP, MARCUS LOPEZ, BEZALEEL SAINZ.