Snowden Overlook
8700 Endless Ocean Way
Columbia MD 21045

DATA PROTECTION, DATA RECOVERY AND CYBERSECURITY ASSESSMENT

Ver 1.0 Nov 22, 2019

Robin Abello
Personal Computerworks, Inc.

Change History

Revision Notes	Date
1.0	11/22/2019

CONTENTS

EXECUTIVE SUMMARY

The goal of the Assessment is to identify the risks from a Cybersecurity attack and other types of failures that would render the computer operations at Snowden Overlook inoperable. We identified the various risks and how to mitigate and recover if the risk happens.

It was determined at the initial assessment meeting that the data being kept in the Snowden Overlook computers do not contain any sensitive personal information and there are no financial data in the systems. Specifically there are no sensitive personal information stored in the Snowden Overlook computers such as birthdays, social security numbers, credit cards numbers and passwords to online accounts. Therefore, the goal of the assessment is to focus on identifying the risks that would affect the normal day to day computer operations at Snowden Overlook.

RISKS

Risk Identified	Risk Control	Recommendation
Desktop Computer Inoperable due to - Mechanical failure - Software failure - Virus infection - User error - Computer stolen	- Computer file backups (Carbonite). - Regular maintenance of computers a. Christy's hard drive was recently replaced. b. OS is kept up to date - [17] Admin access to computers is restricted --- Christy and Carol use a non-admin user account. - [7] OS and apps on the computer are kept up to date - [19] Antivirus/Security software on the computers kept up to date - Office is locked at night and there are security protocols in place to reduce risk of a break-in - [11] Upcoming Cybersecurity training for Christy and Carol	- Do a full computer [3] hard drive backup (at least one and keep offsite). - Add another cloud [13] backup (dropbox) in addition to the Carbonite backup for backup redundancy --- important because o Carbonite's selective file type backup policy. [14] - Use dropbox to sync the shared folder between both computers so if one fails, the other computer can take over some of the tasks of the failed computer. - Have a policy on when [9] to replace the computers (recommendation is to not keep the computers for more than 7 years). - Annual tech audit of [22] computers - Annual security audit [23] to review and identify (new) risks
WinDSX Program in Carol's computer will stop working due to an OS upgrade or her [1] computer becomes inoperable and we cannot reinstall the software --- the software is no longer supported by the vendor.	Discussions with the Vendor on upgrading the software	Upgrade the software so it [2] can be used on both computers (for redundancy in case one of the computers fails). If this upgrade cannot be completed soon (within 90 days), do a full drive backup of Carol's

		computer.
Password file and master password (for the file) can be lost if there's a fire in the building	Dennis and Robin both have copies.	• Store a hard (or soft) copy with the management company --- and update this copy when a password change is made. 5 • Copies to Robin and Dennis should also be updated when a password change is made.
Other tech equipment inoperable due to: 15 • Mechanical failure • Software failure • Virus infection • User error • Stolen	• Vendor will fix internet access issues • Documentation on router configuration • Security protocols in place to reduce risk of a break-in	Replace tech equipment on recommended intervals (10 years for routers and switch equipment). 9
Unauthorized Access to Computers	• TeamViewer is no longer running unattended	Set a time-out (sleep) policy on the computers (3 hours) 18
Account (internet, phones, website, domain, email, antivirus) renewals are missed	Account that need be renewed yearly are set for auto-renew. Management company stays on top of the notices for the renewals and if there are problems with billing (credit card numbers have changed), the management company is contacted.	Include account status checks in the yearly tech audit. 10
Private and Sensitive data may be stored on the computers	There is no private and sensitive data stored on the computers today	Include in the yearly audit a review of the data that is stored on the computers to ensure that we are not storing private and sensitive data. 25 In the event that stricter privacy laws are enacted in the US, a privacy policy will be created and the residents will be made aware of the policy and asked for their consent.

CLOUD BASED BACK UP

- Carbonite

Continuously running in the background on Christy's PC.

Risks

- Backup process fails to run (crashes, no internet connection, program removed)
- Not all files are backed-up --- Carbonite has a selective file type backup policy --- it will backup standard files like Microsoft Office files, but not video files (this is not a problem for Snowden Overlook)
- Carbonite password --- who has this password?

Mitigation

- Carbonite sends an email to account owner (Christy?) that backup has not been running (need to check frequency of this --- how many days after?)
- Use Dropbox as an additional cloud backup --- use this for the shared folder for syncing between Christy's and Carol's computers. With Dropbox, all the files in the dropbox folders are synced regardless of file type.
- Carbonite password is stored on a password folder at the office, and both Dennis and Robin also have copies of the password file.

Carbonite's backup service is certified and compliant with various privacy related protocols and standards --- https://support.carbonite.com/articles/Personal-Mac-Windows-Carbonite-Certifications

- Data stored in world-class data centers that employ the highest security standards
- Automatic detection and backup for new and changed files
- Carbonite servers are located in carefully chosen world-class data centers that are protected by gated perimeter access, 24x7x365 onsite staffed security and technicians, electronic card key access, and strategically placed security cameras inside and outside the building.
- Carbonite is an automated remote or offsite backup and a key component in any disaster recovery plan that protects against hardware failure, theft, virus attack, deletion, and natural disaster.

Recommendation

Use Dropbox as an additional cloud backup --- use this for the shared folder for syncing between Christy's and Carol's computers. With Dropbox, all the files in the dropbox folders are synced regardless of file type.

Dropbox's service is certified and compliant with various financial and privacy related protocols and standards --- https://www.dropbox.com/security

HARD DRIVE BACKUP

3

We are not currently doing a hard drive backup --- this is a recommendation so we have a full-drive backup that includes app that we can then use this backup in the event that we have to do a full system restore.

Recommendation

Perform a full-drive backup of Christy's and Carol's computers. Store this backup offsite. Only need to do this once, unless there is a significant change in the system (OS upgrade, new version of critical apps). Recommended full-drive backup app is Paragon or Acronis.

VIRUS PROTECTION

Background

Anti-Virus software packages look for patterns in files or memory that indicate the possible presence of a known virus.
Anti-virus packages know what to look for through the use of virus profiles or "signatures" provided by the vendor. Since new viruses are discovered every day it is important to have the latest virus profiles installed. Without this protection, viruses are free to infect your systems. Viruses may cause a variety of problems such as loss or damage to information residing on your network, network interruption and inability of customers to access your system

Spyware/Malware — refers to a category of software that, when installed on a computer, collects personal information about a user without their informed consent. Spyware/Malware may be unknowingly downloaded by users when packaged in a Trojan Horse or systems may be infected by viruses that include a spyware payload. There are significant privacy liability implications due to the information that is being harvested and sent to a third party without the user's consent.

Controls on shared drives and folders — a network share is a location on a network allowing multiple users on that network to have a centralized space on which to store files. Unprotected Windows networking shares can be exploited by intruders in an automated way to place tools on large numbers of Windows-based computers attached to the Internet. Unprotected shares can allow Distributed Denial of Service attacks to occur and are also leveraged to propagate viruses and worms both internally to a network and to other networks. There is great potential for the emergence of other intruder tools that leverage unprotected Windows networking shares on a widespread basis.

Implemented Controls

Anti-Virus and Spyware/Malware

- Activated Windows Defender antivirus on both systems
- Installed Malwarebytes on both systems

- Implemented a process to keep Windows Defender and Malwarebytes programs up to date, utilizing automatic update of virus signatures.
- Advised staff not to open e-mail attachments unless they are expected and from a known and trusted source.

19 Execute anti-virus scans on all e-mail attachments, files and downloads before the file is opened.

- Windows Defender and MalwareBytes

- In an infection is detected, Windows Defender and/or Malwarebytes cleans the infected machine
- Prevents virus and malware infections
- Helps stop ransomware attacks
- Shields vulnerable systems and software from new and unknown zero-day exploits
- Prevents access to malicious websites, command and control servers, ad networks, and
- Antivirus scans are automatically scheduled
- Real time protection is always active against viruses, spyware, and malware for opened files and Web pages

24

ENCRYPTION

There is no file-level encryption on the Snowden Overlook computers. Because there are no sensitive and financial data in the computers, we are not recommending using any kind of encryption on the computers.

Recommendation

If in the future a determination is made that sensitive and/or financial data are going to be stored in the computers, we will recommend turning on file-level encryption on the Snowden Overlook computers.

IN HOUSE TRAINING

Background:

Almost all major reports on the current state of the information security threat environment point to users, who are easily mislead as a leading, if not the leading, vulnerability. As technical network security controls have hardened, attackers have increased their efforts toward sophisticated and effective social engineering techniques. Increasingly well-known threats such as phishing have evolved into more complex attacks such as spear phishing and whaling. The payloads of viruses and Trojan horses which are introduced because of user interaction have also become more damaging.
Implemented Controls:

Have a security awareness training program with the following key elements:

- All employees (Christy and Carol) will attend a security awareness training. This training will provide information on how to recognize and report security threats.
- Periodic alerts and reminders should be provided to alert employees to new threats as they emerge and to maintain vigilance in following appropriate procedures to avoid known vulnerabilities.

11

All 2 employees (Christ and Carol) will undergo this training to be given by Robin Abello of Personal Computerworks, Inc.

EMAIL SYSTEM

We utilize Office 365 as our email service provider. Office 365 has a built-in anti-spam filter and a basic anti-virus filter. Both Christy and Carol use the Outlook desktop app to access their Office 365 emails.

20

Recommendation

Asses the risk of a cybersecurity attack that will erase the email data including contacts. If the loss of email data and contacts is significant, consider doing a backup of both email data and contacts, or just contacts.

WINDOWS AND 3RD PARTY SOFTWARE SECURITY PATCHES

Background

Security patch management — updates or patches are regularly provided by software vendors to fix problems within their products.
Many of these patches fix vulnerabilities, which could be exploited by attackers.

7

Implemented Controls:

Windows OS updates are set on automatic
Automatic update of 3rd party applications whenever possible and appropriate.
Verification of unfamiliar patches by contacting Dennis or Robin to verify if unknown patch notice is valid or illegitimate

REPLACING FACTORY DEFAULT SETTINGS ON NETWORK EQUIPMENT

Background:

Firewalls, routers, VPN appliances, wireless access points and other network hardware have pre-defined "factory default" configurations. Similarly, security related software has default settings which are predetermined by the vendor. There are often inherent vulnerabilities in these default configurations if not adjusted to an operation's specific security requirements. A common problem is that administrative passwords for these devices are not changed from the default. Administrative passwords allow device configuration changes that could be used to disable security. Factory default passwords are easy for attackers to guess and, in most cases, are readily obtainable from published lists for specific manufacturers and models.

Implemented Controls:

Dennis has changed the security settings of the routers in the Snowden Overlook office so default configurations are not used and specific procedures have been put in place for the management of strong administrative passwords for these devices and systems.

15

Recommendation

Have a formal policy regarding the configuration of all network devices and systems.

21

NETWORK (LAN, WIFI)

Snowden Overlook’s network is split it up into two distinct networks --- one for the office/staff and one for the guests. The office/staff network is on a separate router and is not accessible from the guest network. There is no wifi system on the office/staff network so the risk of wifi vulnerability is mitigated. There is a wifi system on the guest network, but since that network is not able to access the office/staff network, it presents no inherent risk to the Snowden Overlook computer systems.

WEBSITE AND DOMAIN

The website is hosted on a shared hosting platform with SiteGround and the domain (snowdenoverlook.com) is registered at Enom. The website content is backed-up every day and a copy of the backup is stored on the cloud (dropbox) and a copy of the backup is also stored by Dennis. The risk identified if the website data was compromised is the calendar of events. With the website backups, this data can be restored within a reasonable time-frame.

6

Recommendation

Have a paper copy of the calendar as the immediate backup of the website calendar

PASSWORDS MANAGEMENT

Snowden Overlook has a password folder where a hard copy document of all the account passwords are stored. This is updated by Dennis when a new password is created or an existing password is updated. This is stored in the Snowden Overlook office and only Christy and Carol have access to it. Robin (Tech Consultant) and Dennis also have access to it when they're in the office.

A soft copy of the password document is also kept by Dennis and Robin has a copy. This soft copy is in Excel and is protected by a master password. The master password is stored on the password folder in the office.

Recommendation

5

The management office should have a copy of the password file (soft copy) as a backup, and also the master password.

ACCOUNTS BILLING AND CONTACT INFO

All billing of accounts is managed by the management company. The Snowden Overlook office does not do any financial transactions. It was not clear to me if this also means that the contact info for the various accounts are also the management company. It is important to figure out all the account contact and billing information so that none of the accounts lapse due to a billing issue (e.g. credit card expiring, account number change), or if the internet is down or the phone systems are down, the ability for the staff to work with the vendors is not limited.

Recommendation

10

Do an audit of all the accounts and contact info on the accounts.

POLICY AND PROCEDURES MANUAL

Snowden Overlook does not currently have a Policy and Procedures Manual.

Recommendation

We recommend creating a manual that will cover the following:

- Configuration policy on all tech equipment 15
- Recovery procedures in case of computer equipment failure 16
- Privacy policy for employees 8