HARBOR BRANCH OCEANOGRAPHIC INSTITUTE
FOUNDATION

MEMO

TO: Audit Committee
CC: Melanie Fernandez, BDO
FROM: Katha Kissman, President & CEO
DATE: October 19, 2018
RE: Question about Cybersecurity from Audit Committee Meeting, 10.9.18

Cybersecurity for a small operation like ours (1 server, 3 PC users) entails specific steps to best guard against intentional or unintentional breaches to our data.

Information Technology

Our IT vendor is:

Eric M. Price
President
Technology Partners
2955 20th Street
Vero Beach, FL 32960
E-mail: eric@techpart.net
Phone: 772.299.5178
http://www.techpart.net

Server Integrity

The most important aspect of our cybersecurity is to protect the integrity of our network and our data. Toward that end we have an independent server (i.e., we are not part of FAU's computer system) which is located in a locked cage in the Link building (where our offices are located). While we do not have a key; we do have 24/7 access if we need.

There is hardware firewall (Zyxel ZyWALL) between our network and FAU's outside IP reserved for us.

The server has an external back-up drive. We switched that out in 2017 and all data to that date is stored at our IT vendor. These local backups run daily and keep about 3 months' worth of daily image backups. They are also monitored. Cloud backups are also run daily under a separate system to backup just data on \\scans , \\shared, \\sharedtwo data shares.

We do not have “open ports” on our server. These have been closed, including the email port (see below). Therefore, all incoming traffic is blocked.

Individual PCs

We have an independent onsite WiFi system from FAU’s. We have remote access to our server files as long as the server and the individual PCs are powered on. Access is made available using our IT vendors secure remote solution. Each of the individual PCs are plugged into a Battery Backup & Surge Connection unit.

We utilize Office 365 for our email so all email service is cloud-based (via internet) rather than server-based (onsite). Office 365 has built in spam filters. Our IT vendor just informed us of free trainings through them on how to spot fake or malicious emails. We will be taking advantage of this training. At present, we do not open attachments on emails from individuals whom we do not recognize.

Individual office PCs have antivirus software protection (Trend Micro) against viruses, malware, and ransomware.

Each PC is password protected. Passwords are unique to the user and are not shared. Our system prompts a required password change on a regular basis.

Disaster Planning

We follow protocols set by FAU for hurricane preparedness and other disaster-related planning. When needed, we store our server in the campus bunker and we disconnect and cover our PCs with Visqueen and duct tape.

Credit Cards

We do not accept credit card payments except for the following:

- Donations and ***Love Your Lagoo***n Sponsorships may be paid via credit card through our account with Network for Good. We do not operate an independent merchant account and credit card transactions must be made online via their secure portals.

- In the case of the very few times we have hosted an event where a taking credit card payment was optimum (e.g., live or silent auction at ***Love Your Lagoon***) we utilize Square on my phone for processing directly to our bank account.

Insurance

Our Insurance vendor is:

John D'Albora
Risk Advisor
Vero Insurance, a Marsh & McLennan Agency LLC Company
3339 Cardinal Drive
Vero Beach, FL 32963
E-mail: john@veroinsurance.com
Phone: 772-231-2022
www.veroinsurance.com

In our Policy Package document p. 3 of 7, our current Crime Coverages contain the following:

F. Computer Crime

1. Computer Fraud Single Loss Limit of Insurance: $1,000,000 and Single Loss Retention, $5,000

2. Computer Program and Electronic Data Restoration Expense: Single Loss Limit of Insurance $25,000 and Single Loss Retention, $5,000

The definition/explanation of Computer Fraud Coverage is Coverage for loss of money, securities or other property directly attributable to unauthorized and fraudulent entry of data or computer instructions.

From our carrier:

Here are some facts as to why to carry Computer Fraud Coverage:

- According to a survey by Computer Security Institute, the average financial loss due to computer fraud was $289,000. The average loss due to funds transfer fraud was $500,000.
- Pfishing scams, Trojans, key loggers and other techniques allow hackers to gain control of online banking transactions and to circumvent normal online authentication controls.
- Internal controls such as antivirus software, firewalls, and employee training are critical, but not enough for 100 percent protection.
- Specialized Financial Insurance coverages should be purchased to protect against this risk.

Here are a couple examples of potential computer fraud instances and how it could apply:

- An employee of a customer hacked into a company's website and changed the bank routing and account numbers to her own. When the company paid her employer for services rendered, she fraudulently received the funds in her account.

- A former employee used his supervisor's password to enter the insured's unlocked building and gained access to use the supervisor's computer. Using the bank routing number, he activated transactions to receive fake reimbursements allegedly made to the company's customers.
- An organized crime ring gains unauthorized access to your accounts payable in your computer system and alters the bank routing information on outgoing payments. The result: $1 million transferred to the crime ring's account. This coverage reimburses for the direct loss of money, securities or other property.

For the Computer Program and Data Restoration Expense Coverage, here is some additional explanation and instances it could apply:

In today's data-driven world where sensitive information is stored and transferred both on paper and electronically, organizations of all sizes are vulnerable to costly and damaging liabilities from data security breaches that are occurring at alarming — and growing — rates. Whether data is compromised by a hacker, virus, cyber thief, or because of lost or stolen computers, laptops, flash drives, smart phones or dumpster diving, the breaches can have serious ramifications. There are substantial financial costs involved in finding the cause of and remedying a breach, including the cost of notifying customers— now legally mandated by almost every state. The company can also suffer immense damage to its reputation and from the interruption to business.

Coverage for expenses incurred to restore, replace or reproduce damaged or destroyed computer programs, software or other electronic data stored within your computer or communications network directly attributable to a computer violation.

CLAIM SCENARIO: A computer virus damages your operating system software and data. This coverage will reimburse costs for repair and restoration of your computer programs and electronic data.