SAIL Cyber Questions and Answer

Some questions related to this discussion:

1. Do we collect PHI or other personal or financial information on clients?

a. If so, is that kept in a web-based or server-based system?

b. If it's kept in a server, is there a way to lock it away from the web/internet, preventing remote access?

c. If it's kept in a web-based system, how secure is that system?

SAIL is not governed by HIPPA or 42CFR, so I would say no. If someone released all our info on the internet, seems like we'd be ok for the most part. SAIL does collect social security numbers however, so that could be a sticking point as that is something bad guys can use to steal people's online identities.

2. Where do we keep payroll and personnel information?

a. Is that kept in a web-based or server-based system?

b. If it's kept in a server, is there a way to lock it away from the web/internet, preventing remote access?

c. If it's kept in a web-based system, how secure is that system?

Accounting is kept in Quickbooks. It is not a web-based system. Remote access is extremely limited. Remote access is limited to vpn access, with credentials for a limited number of staff. Once vpn is established, another system must be accessed via different credentials to gain filesystem access. Lastly, only accounting and executive staff have access to accounting. Lastly, Quickbooks has it's own password.
We do not store credit card numbers in Quickbooks. There are currently two credit card numbers stored in the safe on the 3rd floor for monthly re-occurring credit card donations. There is one document on the server that is password encrypted with less than six ORCA monthly auto-pay credit card numbers.

3. If "cyber liability insurance" is available, what would the premiums be?

It is available. It covers things like cyber breaches, staff losing laptops with data on them, that kind of thing. The amount it costs depends on the amount of coverage you want.
We have been quoted $1,500 a month with a $2,500 deductible. Insurance policy information attached.

4. What is the value of our information if:

a. We have our backup safe and secure (which would be up to 7 days out of date, but still viable)?

b. We have no backup?

I don't know if I understand the question. Are you monetizing your info based on the amount of staff time it would take to recollect?
Ex. Director (or designee when Joan is traveling) takes a complete backup off-site each week.

5. What is the level of our cyber security now?

a. Could it be increased?

b. What would that cost?

Security can always be increased. We can spend an infinite amount of time and money to be 'secure'. It is my belief that security is not a yes or no thing, but a degree. If you want something truly secure, then you make it not exist. If it does exist, it can never be 100% secure.

6. Are the costs for insurance and/or increased security greater the value of our at-risk information?

There are plenty of additional things that can be done that wouldn't break the bank. For example, staff have been notified to never open an attachment from an unknown person and if they know the person and weren't expecting an attachment, to check before opening. That said, it is very conceivable that a staff member could inadvertently open a disguised/harmful attachment.

7. Understanding that, even with enhanced security, SAIL could be at risk, should we proactively empower the executive director to make a decision to "ransom" our information without additional board action? If so, should there be a limit as to the ransom paid?

The board discussed this at the May 2016 meeting and were not unified on a course of action. One member was adamant that SAIL should never pay a ransom and cited a federal website that gave the same advice. Another member motioned for a $25K cap on the authority of the Ex. Director to pay a ransom if faced with the situation before the June 2016 meeting. This motion was seconded but failed in a voice vote.

8) Also, what is the "back-up" policy? Do we back-up to a cloud server?

Accounting Quickbooks is uploaded to Dropbox ("cloud"). SAIL can't afford the connectivity it would take to store everything online, unless SAIL moves everything and works from the cloud on a day-to-day basis (which we are investigating). The backup policy is probably too much to write in this correspondence. Attached is a document with all the nuts and bolts.

9) Do we back-up when the server is turned off? Are back-ups stored off site (outside SAIL office) at ED's house? etc.

Backups do not function if the servers are off, but the servers are never off. The sites cannot function if they're off. If the servers are off, no work is being done, and there is, nothing new to backup.