Cybersecurity: Protecting Our Funders, Our Clients, and Ourselves
Friday, May 12th, 2017 at Milne Hall 200

Roundtable Findings

**Legal Issues:**

- Varies widely depending on the domain/sector
- Everyone should be capable of taking reasonable steps to protect information, such as TFA (two-factor authorization)
- What are causes of action for a breach? Make sure you have prevention for each: financial, physical, personal, property.
- Investigate cybersecurity insurance
- There should be known protocols for data access, copying, and emailing.
- Conduct “penetration testing” so that everyone knows what to do in case of a breach
- All protocols should be revisited in the face of and following actual events

**Email Best Practices:**

- No fax machines . . . ever!!
- Sending around emails isn’t enough – employees need training! This includes orientation and refresher courses.
- Be sure to have known password policies
- The responsibility to check on compliance will be never-ending
- Employees should have a daily requirement to access email
- There should be an email policy, with reinforcement, and appropriate discipline for violations
- Consider using a web filter like I-prism
- Outboarding
  - Have an auto-response for 30 days to the supervisor
  - All equipment must be returned immediately
We Just Got Hacked:

- Lessons learned from an actual experience with ransomware (x2):
  - 1. Outsourced
  - 2. Found, isolated, quarantined
  - 3. Recovered
- Be prepared to shut your networks down
- It is important to debrief people afterwards to that they understand the infection vectors
- After the attack is not the time to develop procedures for response (though that happened to us)
- Conduct “phishing testing” of employees
- You will always have employees that are great with mission and not-so-great with technology
- There was sharing of the MS-ISAC products and information

We Don’t Have a Tech Person:

- There are always outsourcing options:
  - CIS
  - Google or Amazon
- It is important to understand the risk analysis with the decision to have/not have a tech person
- You could go to a college or university for interns
- You could grow your own expertise (fund education)
- Solicit a grant and effectively convey the threat in the grant language
- Train and educate your boards and executives
- Training and onboarding are necessary to ensure compliance with best practices
- People in the nonprofit world deal with complex problems (“wicked problems”) daily. They are uniquely well-suited to deal with technology problems (with some training)

Healthcare:

- Healthcare in the nonprofit sector is:
  - Long term care, but unclear what is healthcare and what is Personal Health Information – does HIPAA even apply to us?
  - Refugee resettlement connects people with services
  - Government policies and practitioners deal with many areas of security
- Healthcare is moving into non-healthcare specific organizations lie church organizations and refugee resettlement
- SECURITY IS NOT JUST AN IT FUNCTION
- Communication across the organization is KEY
- HIPAA is the primary concern in this area
• Leverage scale by networking across organizations
• IT pushes technology that is new, but it comes in and causes regulatory and security problems
• Speed causes security problems
• Policies need to evolve with technology
• More forums, meet-up groups, and organizations need to be out there more
• It’s difficult to know whom (especially consultants) to trust
• What are the recommendations and best practices so we can move from principle to practice?
• Important mitigation controls
  o Control policy
  o Training
    ▪ More than third party
    ▪ Is this something that can be more broadly available through schools or local organizations?
    ▪ College graduates generally have no clue coming out of college
  o Find funding for resources