Key Points from the BCSC’s November 21, 2016 Cybersecurity Panel Discussion

There are three key risk areas that registrants should consider when assessing and reviewing cybersecurity risk:

1. Technical
2. Physical
3. Personal

1) Technical Risk

- Use encryption on computer systems and any mobile devices
- Use strong passwords and change regularly
- Keep operating systems current with patches and updates
- Think of OS migration if using older systems as they make your system more vulnerable for attacks. For example, Windows XP is no longer supported by Microsoft and be prepared to update from Windows 7 soon
- Keep your software applications to the minimum necessary for your staff to do their job, i.e., don’t install software if you don’t need it
- Do internal testing
- Separate the phone system from the network system and use different vendors for both services
- Consider using “white hat” hackers to test your systems and network security
- Do due diligence to find a reputable vendor to service IT systems
- Use another vendor to test the systems

2) Physical Risk

- Identify information assets and how those assets are stored, e.g., locally, offsite and/or in the cloud
- Disable USB ports to restrict data transfer
- Consider restricting employee access to file-sharing sites and services, such as DropBox
- Auto-lock of computers after screen timeouts
- Escort visitors in the office

3) Personal Risk

- Train staff to understand the risks and dig deeper if any red flags start waving
- Know your client well enough to identify unusual behavior and requests
- Professional skepticism: Ask questions instead of accepting statements or requests at face value
- Call clients to verbally verify suspicious or unusual email requests from clients
- Log all client communication

Suggested Practices

- Cybersecurity insurance

- Backups – keep several iterations of backups off site, because ransomware may lay dormant for some time after infecting a computer
- Disconnect your backup drive from your network and store it off site
- Test the backup periodically – confirm that the data is whole and reliable
- Diversify the backup, such as using tape and hard drive methods
- Use backup servers in a location outside of the local seismic zone to mitigate the risk of disasters and other business continuity events
- Have an action plan so that when an attack happens, you can remediate it quickly