Cyber/Data Security

For Churches

What Risks Does a Church Face?

Risk for ongoing operations

- Day to day activities (communications systems, access to member/donor information)
- Inability to receive and track donations (loss of donations)

Risk to reputation/trust

- Often more costly than just being ‘down’ for a day or two
- Compromised data in one system often means loss of trust in all your systems

Risk of Costly Litigation

- Organizational impact
- Some cases may include individual impact

What needs to be protected?

Sensitive information

- Contact information on members and attendees (addresses, pictures, phone and email). These records usually include information on minors
- Donation information. ACH, EFT, credit card information
- Security data--access to facilities, to computer programs
- Employee data
- Some email, voicemail, text messages contain sensitive data.

Access to software systems

- Logins/accounts/access to the systems that contain the information you rely on
- Member portals/logins to systems by members and attendees

Address the challenge by:

- Assigning someone who will be responsible for follow through/reporting
- Understanding what you have that needs protection
- Knowing where the data actually is
- Leveraging resources you already have
- Working with vendors
- Training staff
- Making a plan

Assign the task

- The church can be held legally responsible for various types of cyber/data breaches
- Identifying someone who can follow through and report status increases the likelihood that it will happen
- Although a person or persons may be assigned this task, some part of the church's administration has to
    - Support these activities
    - Determine what acceptable risk levels are for the organization
    - Direct the agreed upon changes
    - Sustain the effort as volunteers change

Understand what you have:

- Inventory the systems you use (include phone systems, physical security systems, online or SaaS systems (directories, donations), mobile apps, etc.)
- Know who uses them and who is in charge of administration (creating logins)
- Review the type of data is in them--sensitive, does it fall under any regulations?
- Identify procedures that are in place to ensure that those who need the data have access and those who don’t need the data in their work, don’t have access
- Is there functionality built in the system that is or could be leveraged to increase security

Understand where the data actually is:

Are the systems you use on servers in a church closet?, at someone's house?, are they in "the cloud"? Do you keep all the data in the system or do some folks store copies of information (reports, lists) on their computer as well.

The location impacts your options and responsibility for protecting it.

- If you can touch the device(s) where the information resides, you have the responsibility to protect the physical devices. This includes firewalls, operating system patches, antivirus, etc.
- Even if the data resides in the cloud and you simply access it, you are responsible to ensure that user accounts are not compromised and to vet the vendor's security program to ensure that it is adequate for the type of data that is being stored.

Leverage what you already have:

- Within the configuration settings of software that you already use, enforce long passwords, and require password changes on a regular basis
- If systems can be configured to use 2 Factor or Multi-factor authentication--enable it.
- Don’t allow users to share their access credentials (this may cost more in licenses but that is a small price to pay compared to the cost of a single breach).
- Clean up accounts--get rid of (disable, deactivate) accounts that are not actively being used.
- Set up all devices (laptops, desktops, tablets, phones) to require a login with a password or PIN.
- If encryption can be enabled. Windows has a product called bitlocker that can be put in place to encrypt hard drives. In some software programs, it is possible to put special encryption on specific fields.
- Make sure that if/when vendors put out security patches (for operating systems or for their programs or hardware), the patches get applied.
- Set antivirus and antimalware scans to happen on a regular basis

Consider the following:

- Using a single sign on tool. Both Google and MS Office 365 have these tools. There are also tools like LastPass that can be used to remember your passwords so that you only have to remember one.
- Adding email encryption to be used by individuals if they need to send emails with sensitive information outside of your domain or if you don't have email under a church-specific domain. One example of this type of software is Zixmail.
- Consider purchasing cyber security insurance.
- Consider contracting with a local tech company to ensure that your hardware and operating systems are patched on a regular basis
- Creating policies for using church systems, equipment, and data.
- Having counsel request a security report or audit at least once each year.

Work with vendors to

- Upgrade when software applications or operating systems are no longer supported. Unsupported systems are highly vulnerable.
- Find out what they offer that could enhance security (WIN OS bitlocker, Office 365 Single Sign On, Google Identity Manager, Google Mobile Device Management)
- If you have vendors that store credit card, bank information, or any sensitive data, ask for a copy of their security certifications on an annual basis
- Understand your responsibility in letting vendors know if something seems amiss in your data
- Be certain you know what their contractual obligations are related to telling you if they have experienced a breach
- Make sure that your vendors know you are a 501(c)3 or Charitable organization and press them for non-profit/charity pricing.

Learn/Train

- How to recognize and respond to various types of cyber threats
  - Phishing
  - Voice phishing
  - Ransomware
  - Malware
- Best practices re
  - (not) sharing accounts
  - Different passwords for different systems
- On the plan for reporting and responding to a suspected or possible breach

Create a Plan

- Create a plan for dealing with potential situations such as a data breach or a compromised system.
  - Do people know who to inform of a breach or a suspected breach?
  - Who will be responsible to deal with the vendor(s), authorities, members if/when you have a data breach?
- Review resources.
  - If the church has cyber insurance, that insurance may include technical and legal assistance in responding to a breach.
  - Identify reputable vendors that could help and compile a list (review annually).
  - Are there members in your congregation that could be technical or legal resources?
- Task a specific individual with staying aware of what your state/province and federal laws are

Resources:

(this list is not exhaustive)

- National Institute of Standards and Technology, Small Business Information Security Foundations (worksheets to help you gather the information and evaluate your risk).
- Evaluating your vendors--a paper by J.P. Morgan
- Free staff training in cyber security.
- Security information on vendors that process credit cards (look for your vendors on the lists that are linked here).
- Free antivirus/malware software
- Current Security News
- Canada specific resources
    - Canadian charity law and risk information (look under the Publications and Resources section).
    - Canada's Personal Information and Protection and Electronic Documents Act PIPEDA
- US government resources
    - Cyber Security (US Gov Cyber Security for Small Business--applies to churches as well)
    - Cyber Security Resources for Non-profits
    - Data Privacy
- Provincial/state government websites will lead you to **laws specific to your location**.
- The UK has a nice summary in their National Cyber Security Centre's Tips for Charities