GC Mandated Cyber Insurance Requirements

Information based on Adventist Risk Managment Webinars
https://vimeo.com/721114965/dc85b5269c
https://vimeo.com/723083311

Yikes Statement

Due to rising cases and costs of cyber fraud the GC is now requiring by policy that all organizations carry cyber insurance.

Some conference will be purchasing cyber insurance which will cover their school AS LONG AS those school follow the Conference guidelines.

Check with your Conference regarding cyber insurance.

Sounds a little scary, daunting, and time-consuming doesn't it?

Good news: If properly prepared, recovery from a cyber breach would only require restoring/rebuilding what is lost. Recovery could be quick and Cyber insurance may not be needed beyond possibly providing funds.

Bad news: If sensitive data is stolen/ransomed, recovery becomes complicated, and even worse – cyber insurance may deny the claim if guidelines were not being followed. Financial losses can be astronomical! —Uh-oh!!!!

Here is our approach...

Ease into it. Be DELIBERATE!

- There are 7 required items. Plus one critical step
- Timeline to implement: Due sometime this school year and ongoing thereafter.
- Use your creativity to find the easiest route for you.
- Start with the most critical needs first.

1. Multiple Factor Authentication

Whenever possible turn on MFA for devices and subscriptions that access sensitive data.

- ➔ **Devices**
  Example: Work phone, treasurer's computer.
- ➔ **Online Subscriptions**
  Example: SIS (FACTS/Jupiter)
- ➔ **Critical Data**
  Example: Banking

Tip

- Usually students don't need this.
- Treasurers need this.
- The closer an employee is to sensitive personal information the more they need this.

2. VPN Encrypted Connection

When away from the school use a VPN software connection if you connect from a phone/computer into your school network to access sensitive information.

- ➔ **Hardware**
  Example: School security cameras.
- ➔ **Finances**
  Example: Financial documents on a drive.
- ➔ **Student Documents**
  Example: Court order, Application, copy of birth certificate, Personal information

Tip

No school network. Don't worry about this at all.

If you have a school network and no personal data on it, probably don't worry about this.

3. Cyber Security Training

At least once a year offer cyber security training for staff and students.

- ➔ **Subscribe to a vendor**
  Example: KnowBe, NINJO
- ➔ **Course**
  Example: Take a course on ALC
- ➔ **Teach**
  Example: Have the technology person/director talk about how to recognize suspicious emails and safely use the internet and avoid risky web links.

4. Critical Patches & Updates

Every two months (at minimum) update all phones, computers, and infrastructure hardware with the latest patches and updates.

- ➔ **Turn on Auto Updates**
  Example: Have your computer automatically set to update the latest patches and updates.
- ➔ **Manually Update if no auto**
  Example: Create a document to track last time updates were done.
- ➔ **Designate someone to check**
  Example: Volunteer or employee verify.

Tip

If you incur a cyber breach and have no sensitive personal data on computers, there won't be a need for an insurance claim...

You'll be crying though!

5. Malicious Email

Only use the organization email for work. Most conference have you covered to protect you from malicious email.

- ➔ **Don't use personal email**
  Example: Home email account.
- ➔ **Don't share your email password.**
  Example: None needed here… right?
- ➔ **Try to use trusted devices to access work email.**
  Example: Use devices you know have virus protection.

6. Virus Protection

Ensure that all devices that access sensitive data (especially finances and student's personal information have antivirus, anti-malware, and endpoint protection.

- ➔ **Virus Protection**
  Example: Purchase a subscription. Turn on auto update and auto scan.
- ➔ **Firewall**
  Example: Turn on device firewalls. Keep school firewalls updated.
- ➔ **Internet Filtering**
  Example: Install on all school devices.

Tip

You should make employee devices the number one priority if you are on a budget.

7. Backup Critical Things

Backup critical files periodically especially for sensitive and critical files. Keep backup in fireproof safe offline.

- ➔ **Designate Someone and Verify**

  Example: Check and verify that backup copies are valid and can restore fully.

- ➔ **Use a thumb drive/portable drive**

  Example: Backup your most critical folders and confirm they open.

- ➔ **Rotate Backups**

  Example: Keep more than one copy.

Tip

You might as well grab your administrative files like the school handbook, application forms, etc. while your at this.

No need to cry if you have a current backup.

KEEP OFFLINE COPIES of LESSON PLANS!