Cybersecurity For Association Chapters: 5 Best Practices

Your members are focused on cyber security, both at home and at work. They have antivirus software on their computers, complete cyber quizzes at work (“what is phishing?” sound familiar?) and may even require a password for their home wireless internet. Are you applying a similar level of security and security awareness to the systems and data associated with your chapter? Think about your member, member guest, sponsor and overall chapter data; the combination of that data and your (often) limited resources needed to manage it all can make your organization an easy target for cybercriminals.

It’s easy for thieves, for example, to send an email to your treasurer and make it look like it’s from the chapter president. That email could ask the treasurer to pay a bill electronically; the bill might even look like one the chapter normally pays. So, the treasurer clicks on the link in the email or opens an attachment. They think they’re paying the bill, but they’re actually paying the thieves. Or, worse, they click on the link and the thieves hijack the chapter’s bank account, and all the chapter’s money drained from the account.

Regardless of a chapter’s size, cyber security needs to be a priority. You can easily apply a few cybersecurity best practices to your association chapter, to keep your data secure and all your stakeholders trusting you with their information.

5 association chapter cybersecurity best practices

Maintain a current chapter cybersecurity policy. To ensure that everyone connected to the chapter is equally focused on its security, you need a policy that covers your guidelines and procedures for protecting chapter data and systems. A chapter cyber policy should include things like password management; data encryption; incident response; and member, staff and board member security training. It's also important to know that as thieves' methods continue to evolve and improve, chapters should regularly review and update their chapter cyber policies.

Educate your members and other stakeholders. Your entire chapter is responsible for cybersecurity, not just your board or your VP of Technology; this requirement should extend to your general membership as well as your sponsors and vendors. Hold regular cyber security training for your board and your members that illustrates, using real-world examples they can easily understand, topics like recognizing and responding to potential cyber threats, as well as the importance of strong passwords, phishing awareness and safe browsing habits. Outside of training, remind people of the importance of cyber security to the chapter's security and make it more engaging by showing them how they can apply these same tactics at home and at work. Consider mentioning important points in Cyber Sessions during your monthly meetings and sending out tips in email and in your chapter newsletter.

Implement access controls. Unauthorized access to data can have severe consequences. Require board members, staff and members to use unique usernames and passwords, and consider multi-factor authentication (MFA) when possible. Regularly review access for board, committee and general chapter members, and eliminate access for those who no longer need it, like members who've left and board members who have stepped down from their roles, and don't forget your former chapter accountant. They definitely no longer need access! And limit access to only what a person needs. Does your VP of marketing really need to see your financial statements? Maybe, or maybe not. Review your access levels regularly and adjust them as necessary.

Backup your data regularly. Losing data for any reason, cyber or technical, can be devastating. Think of all the time and money your chapter could lose if your chapter web site is hijacked. Regularly backup your critical data and systems and store these backups in a secure location, either offsite or in the cloud. Test your data restoration process periodically to ensure the backups continue to work correctly.

Secure your infrastructure. Before visiting your chapter website or other systems, your users need to know these systems are secure, especially when they access them from their home or office. Consider encrypting your sensitive data and systems used by chapter members. Encryption secures data by taking information, like text or files, and "scrambling" it. This makes it unreadable to anyone without proper authorization, even if it's intercepted or accessed by someone else. Using firewalls, intrusion detection systems and secure routers are additional ways to safeguard your chapter network.

Give Chapter Members Easy Ways to Ask for Cybersecurity Help

It's easy to spoof an email address or a web link to make it appear to – but not actually – come from the chapter. Anyone with questions about an email from a sender they're not sure about, a link that looks the slightest bit unusual, etc. should feel comfortable asking someone in your chapter what they should do, before responding to an email, opening an attachment or clicking on a link. Create an email address or have a phone number for members, vendors, sponsors, etc. to use for questions about chapter cyber security.

There can be serious implications when a chapter system gets hacked. Having a chapter cyber policy and controls in place can keep your chapter and those you interact with safe and secure.