CYBER LIABILITY EXPOSURES

The U.S. Congressional Small Business Committee found that 71% of cyber-attacks happened at businesses with less than 100 employees. Even more concerning is the fact that the 2016 State of SMB Cyber Security Report by Ponemon and @Keeper found that 50% of SMBs have had a security breach in the past year. A vast majority of fraternal organizations fall within this business category with less than 100 employees. As such, fraternal organizations have been and continued to be vulnerable to a security breach.

Fraternal organizations have specific cyber liability exposures arising out of the use of their websites, electronic communications, Facebook Pages, and collection of member personal identification information which in some cases includes collection and storage of member social security numbers and credit card numbers. Because of these exposures, we believe fraternal organizations should consider adopting a set of Best Practices which are intended to minimize the probability of a security breach occurring and reduce a number of issues the organization would face.

CYBER LIABILITY BEST PRACTICES

Taking fundamental steps to protect your system and the data contained on it, can reduce the probability of a successful cyber-attack; saving the organization direct and indirect expenses as well as disruption to the normal business activities of the organization.

Educate all Employees: It is essential that employees accessing the network be properly trained on your organization's network security policies. Since policies evolve as cybercriminals become savvier, it is important to have regular updates on new protocols that are put into place. To hold employees accountable, have each employee sign a document stating that they have been informed of the policies and understand that actions may be taken against them if they do not follow the security policies.

Use of a Firewall: One of the first lines of defense in a cyber-attack is a firewall. The Federal Communications Commission (FCC) recommends that small businesses, including fraternal organizations, set up a firewall to provide a barrier between your data and cybercriminals. In addition to standard external firewalls, many organizations now install internal firewalls to provide additional protection. It is also important that employees working from home install a firewall on their home network as well. We recommend that our clients consider providing firewall software and support for home networks to ensure compliance.

BEST PRACTICES CONTINUED

Encrypt Data and Portable Media: Firewalls are not perfect. If a hacker manages to get through your firewall and into your network, your data is vulnerable. Encryption will make data unreadable to the hacker. Consider using an encryption program to keep computer drives, files, portable media devices, and even email messages safe from hackers.

Regularly Back Up all Data: Regardless of all precautions you may make, the possibility of a breach exists. Therefore, backing up word processing documents, electronic spreadsheets, databases, financial files, account receivable files, and account payable files is critical. Be sure to back up all data stored on the cloud. Make sure backups are stored in a separate location due to the possibility of flood or fire damage occurring.

Install anti-virus, anti-malware and anti-spyware software: This loss control technique is the easiest and most effective way to increase security at your organization. Make sure to install the software on each computer in your network—computers that don't include these types of software are much more likely to be exposed and can possibly spread malware to other computers in the network. There are a host of viable options for each type of software, ranging in price from free to an annual subscription. Be sure to keep the software as up-to-date as possible. Do not assume that employees will never open phishing emails. The Verizon 2016 Data Breach Investigation Report found that 30% of employees open phishing emails. Since phishing attacks involve installing malware on the employee's computer when the link is clicked, it is essential to have anti-malware software installed on all devices and the network as well.

Enforce Safe Password Practices: While changing passwords may be viewed as inconvenient by employees, it is an important practice to follow. The Verizon 2016 Data Breach Investigations Report found that 63% pf data breaches occurred due to lost, stolen or weak passwords. Given the fact that employees typically purchase their own device, it's essential that employees accessing the organization's network be password protected. We recommend that employees be required to use passwords with upper and lower case letters, numbers and symbols and that password changes be required every 60-90 days.

BEST PRACTICES CONTINUED

Use Multifactor Identification: Even with proper preparation, the odds remain high that an employee will likely make a mistake that can potentially compromise your data. As a result, using multi-factor identification settings on most major network and email products is simple to do and adds an extra layer of protection. Review your network settings and require every employee to enter their cell phone number as a second factor. If this is done and a cybercriminal steals the employee's password, they cannot use it unless they also steal the cell phone and know the PIN as well.

Use a Virtual Private Network (VPN): A VPN allows employees to connect to your company's network remotely. VPNs eliminate the need for a remote-access server, saving fraternal organizations lots of money in remote server costs. In addition to these savings, VPNs also provide a high level of security by using advanced encryption and authentication protocols that protect sensitive data from unauthorized access. If your company has salespeople in the field or employees who work from home or away from the office, a VPN is an effective way to minimize cyber risks.

Properly Dispose of Sensitive Data: Create a policy regarding the deposal of sensitive data, regardless of the storage medium. The policy should include instructions for paper documents and files along with any electronic files, documents or media. Devices and equipment no longer in use should be securely wiped to remove all sensitive information.

Review Third-Party Vendor Contracts for Security Requirements: An organization's cyber security posture is only as strong as that of its vendors. Approximately 30% of data breach incidents received by Cyber Liability carriers have been traced to a third-party. As a result, organizations must evaluate the cyber security exposures of their third-party vendor relationships. Selecting vendors that go through regular audits to evaluate their information system security, integrating security requirements and standards into any vendor contract, and outlining responsibilities of all parties in the event of an incident that include notification procedures and timeframes are all steps to reduce third-party risk.

Plan for Mobile Devices: With the increasing popularity of mobile devices with wireless capabilities, it is important to extend the security policies of the organization to employees utilizing these types of devices for business purposes, which include the following:

BEST PRACTICES CONTINUED

- **Establish a Mobile Device Policy:** Before issuing smartphones, tablets or other mobile devices, establish a device usage policy. Provide clear rules about what constitutes acceptable use as well as what actions will be taken if employees violate the policy. It is important that employees understand the security risks inherent to smartphone use and how they can mitigate those risks.

- **Establish a Bring Your Own Device (BYOD) Policy:** If you allow employees to use their personal devices for company business, make sure you have a formal BYOD policy in place. Your BYOD security plan should also include installing remote wiping software on any personal device used to store or access company data, educating and training employees on how to safeguard company data when they access it from their own devices and informing employees about the exact protocol they must follow if their device is lost or stolen.

- **Keep the devices updated with the most current software and antivirus programs:** Software updates to mobile devices often include patches for various security holes, so it's best to install the updates as soon as they're available. There are many options to choose from when it comes to antivirus software for mobile devices, so it comes down to preference. Some are free to use, while others charge a monthly or annual fee and often come with better support. In addition to antivirus support, many of these programs will monitor SMS, MMS, and call logs for suspicious activity and use blacklists to prevent users from installing known malware to the device.

- **Back Up Device Content on a Regular Basis:** Just like your computer data should be backed up regularly, so should the data on your company's mobile devices. If a device is lost or stolen, you'll have peace of mind knowing your valuable data is safe.

- **Choose Passwords Carefully:** The average Internet user has about 25 accounts to maintain and an average of 6.5 different passwords to protect them, according to a recent Microsoft study. Obviously, this lack of security awareness is what hackers count on to steal data. Require employees to change the device's login password every 90 days. Passwords should be at least eight characters long and include uppercase letters and special characters, such as asterisks, ampersands and pound signs. Don't use names of spouses, children or pets in the password. A hacker can spend just a couple minutes on a social media site to figure out this information.