HOW ASSOCIATIONS CAN IMPLEMENT BETTER CYBER HYGIENE PRACTICES AS EMPLOYEES WORK REMOTELY

A combination of employee training and cyber liability insurance can help protect your association from nefarious cyber actors as more employees work from home during the COVID-19 pandemic.

Are you finding yourself washing your hands more, not touching your face as often, remaining six feet apart, or even wearing a face mask? These are just a few best practices the world has adopted to fight the spread of COVID-19.

As many of us find ourselves working from home for the foreseeable future, we must adopt similar cyber hygiene practices for the health and safety of our associations. Like viruses lurking on an uncleaned surface, bad actors are seeking to exploit this new working environment to pursue their nefarious cyber agendas. Associations must understand the extent of the problem, train staff to combat it, and be sure their cyber insurance is updated to cover remote work.

The Problem

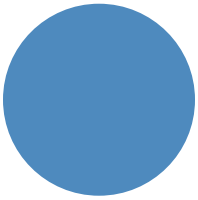
As association professionals work from home, not only are they moving fast, but they are also dealing with numerous distractions, including children learning remotely, spouses working alongside them, and their own fears and anxieties about the virus itself. "Some are using their own personal devices and others are working with company resources," said Joanne L. Martin, cybersecurity advisory practice lead at Hartman Executive Advisors. "Systems continue to be secured in many instances; however, remote employees need to be especially mindful of cybersecurity during these times and slow down to make sure they're not inadvertently responsible for a preventable data breach."

Jen McPhillips, director of business operations at Coalition, a cyber insurer, noted recently that "exploitation of remote access points and services is the root cause for over 40 percent of all ransomware claims reported to us. … [C]yber criminals are already exploiting the changes organizations are implementing to facilitate remote work and launching phishing campaigns to exploit mass uncertainty and fear."

Staff Training

Erik Haas, director of sales and marketing at designDATA, a managed-IT services firm, noted that "bad actors are customizing their phishing schemes to exploit" the current remote working conditions.

"Haas said the 'human firewall' is the most important asset in defending financial and digital assets. Associations must commit to regular cybersecurity training for staff that helps them employ the right behaviors and that they become second nature."



Derek Symer
Partner | 202.845.8260 | Derek.Symer@ahtins.com
AHT Insurance - A Baldwin Risk Partner

AHT INSURANCE
A BALDWIN RISK PARTNER

Haas said the "human firewall" is the most important asset in defending financial and digital assets. Associations must commit to regular cybersecurity training for staff that helps them employ the right behaviors and that they become second nature. Good training transforms "shouldn't have clicked" into "shouldn't click."

Haas offered some basic measures that organizations should take to improve their cybersecurity posture:

- use of a VPN
- multifactor authentication
- unique passwords of sufficient length
- vetting links and attachments before clicking
- keeping patches and backups up to date
- training, training, and more training

Cyber Liability Insurance

So, what happens if the training and IT changes aren't enough and there is a breach or hack of your association? That's where cyber liability insurance comes in. Associations need to make sure their policy offers clear coverage grants for remote workers, employee-owned devices, and even outsourced IT partners.

Every cyber insurance policy is like a unique flavor of ice cream, and the devil is in the details when it comes to coverage for teleworkers and remote login points on a network. A best practice would be that associations double check the provisions of their cyber insurance policies to make sure they have the coverage for the new remote working reality and to ensure they have affirmative coverage as it pertains to teleworking employees. Most cyber policies worth their salt will have this coverage already baked in.

While some have found increasing other types of insurance difficult during the COVID-19 era, this is not the case in cyber liability. Even if you need to increase your limits or amend coverage (if insufficient), it should be relatively easy.

So, what are some key takeaways? First, leadership needs to mandate strong passwords on local networks and using VPNs wherever available for connecting to work systems. Consider implementing a password-generating platform, if feasible. Leaders should also reinforce training and frequently remind employees to be on the lookout for phishing attempts. Everyone is moving so quickly and trying to accomplish a great deal under difficult circumstances, but one wrong click could lead an association down a disastrous path. Finally, check your cyber insurance coverage. Extra caution is required from each employee, but guidance needs to come from the top.