CYBERRISKS+LIABILITIES

July/August 2018

IN THIS ISSUE

hierl

Save Your Website from ADA Lawsuits

The Americans with Disabilities Act (ADA) of 1990 prohibits discrimination based on disability, which involves ensuring that everyone has reasonable access to all areas of public life. Although the ADA doesn't explicitly mention the internet, the federal government has taken the position that Title III of the ADA covers access to websites of public accommodations, including service and rental establishments, retail stores, educational institutions and recreational facilities.

Currently, ADA website compliance is only mandatory for government-managed websites. However, the absence of laws enforcing ADA compliance for websites of public accommodations hasn't prevented people from filing lawsuits against companies that don't meet the suggested guidelines.

Businesses in health care, government and education have been the most common targets of these lawsuits. Attorneys looking for easy money typically target small businesses' websites by offering a low settlement fee. If your business is targeted by an ADA website compliance grievance, consider taking the following steps in response:

1. **Review the grievance for credibility.** A lawsuit may likely begin by citing "violations of the Americans with Disabilities Act, Title 42 U.S.C. 12101 and 12181." It may also include an inexpensive settlement option—a prime indicator that the lawsuit has no legs to stand on and is likely a scam.

2. **Consult a lawyer.** Doing so will help determine the credibility of the threat and stop future threats to your business.

3. **Respond to the plaintiff.** Ask your attorney to draft something explaining that you've reviewed their grievance and consulted a lawyer. Realizing that you've sought legal help may scare away anyone trying to file a lawsuit.

4. **Update your website.** Do this regardless of whether there is a legal need. If your site is easily accessible by people with disabilities, you may see beneficial returns from those users.

Training Staff to Guard Against Cyber Attacks

Using mobile devices to work remotely is becoming the new norm. But when your employees use phones, tablets and laptops to access your network and do their jobs, they're essentially providing hackers with more entry points, leaving your organization highly vulnerable to attacks.

No matter how many security measures you take, they're useless if you don't supplement them with employee training. Here are five ways to help employees protect your company from cyber attacks:

1. **Offer training on phishing and spam**. Show your employees what to look for so they can alert IT if they receive a suspicious email. You can also use phishing simulator training tools, which attempt to trick your employees into opening the wrong types of email. The employees who click on those emails can then be flagged for additional training.
2. **Provide strong password training**. Passwords should be changed on a regular basis and contain more than seven characters, an uppercase letter, a number and a symbol.
3. **Teach employees to report problems**. Even if your employees clicked on something they shouldn't have, it's important that they feel comfortable reporting their infractions so any potential threat can be addressed immediately.
4. **Insist that your employees update all software when new updates become available.** Vulnerabilities spread like wildfire among hackers. If employees fail to perform updates, they're allowing hackers access to the device and possibly your entire network.
5. **Give remote access and Wi-Fi training and set up a virtual private network (VPN).** Any employee that works remotely should use that VPN at all times for all activities.

Businesses Need Both Cyber Threat Intelligence and Business Risk Intelligence

Devising an all-encompassing strategy that protects your organization from cyber criminals, data breaches and other cyber security threats is no easy task. You need to ensure protection from not only hackers, but also the actions of your own staff.

Your employees may not intentionally threaten your organization, but without proper training and policies on using, storing and transferring data, there will always be a chance of them inadvertently putting your business at risk. In order to protect against such threats and react accordingly, businesses need to two types of intelligence: cyber threat intelligence and business risk intelligence.

Cyber Threat Intelligence

Cyber threat intelligence is information that has been collected, evaluated and analyzed. It involves looking outward, always being on the defense for potential cyber threats and turning unknown threats into well-known, mitigated threats. Cyber threat intelligence helps organizations understand the threat landscape they face and improve the effectiveness of their defense.

Cyber security analysts can use the data from their own internal security systems and outside vendors to build an understanding of the threats they face. They may also enlist the help of outside providers who understand the behavior of cyber criminals, as well as the long-term trends and short-term risks that might affect a particular sector.

Business Risk Intelligence

Business risk intelligence addresses the broader risks facing a business, including the digital risks. Due to the connected nature of the "internet of things," business risk intelligence can also include cyber threat intelligence. But unlike cyber threat intelligence—which primarily affects the day-to-day operations of a company's chief information security officer—the impact of business risk intelligence is likely to be felt across the entire executive suite.

A company with business risk intelligence is aware of the broad risks it faces. That may include insider threats to the physical security of staff or the risk of engaging with third-party vendors in the supply chain. Any type of activity that can alter business operations can be combatted with business risk intelligence.

Hierl Insurance Inc.
325 Trowbridge Drive
Fond du Lac, WI 54937
920-921-5921
www.hierl.com