ACRISURE®
LAW FIRM SOLUTIONS

Tip of the Month

Brought to you by:

ZYWAVE
INSURING GROWTH

XL

LACBA
LOS ANGELES COUNTY BAR ASSOCIATION

Acrisure (rebranded from AHERN Insurance Brokerage in 2024) is the Los Angeles County Bar Association's Preferred Professional Liability Insurance Broker since 2008, is one of the largest and most respected full-service insurance brokers in the country specializing in insurance for law firms.

Acrisure is pleased to offer LACBA members an exclusive Professional Liability Program with AXA XL.

Call (800) 282-9786 to speak with an Acrisure Professional or visit us online at www.acrisure.com/ahern.

Cyber Risks & Liabilities: 5 Cybersecurity Controls to Implement in 2024

As the new year begins, there are several ways for businesses to bolster their digital defenses and minimize potential cyberthreats going forward. Here are five essential cybersecurity controls that organizations can implement in 2024 to help manage their digital exposures:

- 1. Utilize multifactor authentication (MFA). MFA is a layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify their identity for login. It's best for organizations to enable MFA for remote access to their networks and any enterprise level cloud applications.
- 2. Leverage patch management solutions. Patches modify operating systems and software to enhance security, fix bugs and improve performance. Patch management refers to the process of acquiring and applying software updates. A consistent approach to patching and updating software and operating systems helps. limit exposure to cyber threats.
- 3. Install email authentication technology. This technology monitors incoming emails and determines the validity of these messages based on specific sender verification standards. Such technology can make all the difference in keeping dangerous emails out of employees' inboxes and putting a stop to cybercriminals' tactics before they begin.
- 4. Have a plan. Cyber incident response plans can help organizations address digital threats, remain operational and mitigate losses in a timely manner amid cyber attacks. Successful plans should outline potential attack scenarios and methods for maintaining or restoring key functions during these events.
- 5. Provide training. Employees are often organizations' first line of defense against cyber incidents; all it takes is one staff mistake to compromise an entire workplace system. As such, it's crucial for organizations to offer routine cybersecurity training.

Contact us for more risk management guidance.

ACRISURE®
LAW FIRM SOLUTIONS

Tip of the Month

Brought to you by:

ZYWAVE
INSURING GROWTH

XL

Understanding and Preventing Shoulder Surfing

Complex and high-tech cyberattack methods often garner a significant amount of attention. However, businesses must also remain vigilant against older, relatively simpler tactics like shoulder surfing. This attack method can be conducted through no-tech means (e.g., someone peeking over an employee's shoulder and writing notes on what
they see), low-tech means (e.g., a malicious actor using binoculars to peer at classified information from a distance) or high-tech means (e.g., a cybercriminal using cameras to surreptitiously record confidential data displayed on a screen).

If an employee is a target of a shoulder surfing incident, several consequences may result. The perpetrator may gain unauthorized access to the business's payment systems, confidential client information and intellectual property. In addition to compromising business data, the malicious actor could steal the employee's identity and, subsequently, make unauthorized transactions and commit other forms of fraud. These events could lead to costly regulatory penalties and fines, high investigation and remediation expenses, lawsuits and reputational damage that erodes trust with clients and partners.

Considering the impacts that shoulder surfing can have, businesses should take steps to prevent this type of attack from occurring. Strategies to consider include the following:

- Provide regular employee education and training. Businesses should educate employees about the threats and impacts of shoulder surfing and train them on how to reduce the risk of being the target of such an attack.
- Implement physical security measures. Several types of physical security measures, such as screen protectors and privacy filters, can be utilized to hinder shoulder surfing. Businesses can also arrange their workplaces so private information may not be viewable by unauthorized parties.
- Utilize technological solutions. Technological safeguards can be implemented to reduce the risk of shoulder surfing attacks. Businesses should consider using tools such as MFA, biometric authentication, encrypted communication channels and password managers.

Contact us today for additional cybersecurity solutions.

San Diego Corporate Office
1615 Murray Canyon Road, Suite
1050, San Diego, CA 92108.

Toll Free | 800.282.9786
Telephone | 858.571.9030
Fax | 858.571.9010

ACRISURE.COM

CA LIC 0K07568 | AZ LIC 1800012964