SafeAlert®

Loss Control Advisory Bulletin from ABA Insurance Services

Be sure that BYOD protocols are in place

In order to move your employees to a remote work environment quickly and efficiently, your organization may have allowed employees to use their own personal devices while out of the office, such as their home computers, tablets and/or cellphones. This is commonly known as BYOD or bring your own device.

Your organization may already have BYOD policies and procedures in place. If not, these policies can add another layer of protection to your systems, enhance data security, and protect your own employees' devices and information.

Some BYOD recommendations:

- Approved devices should be new enough to support current and ongoing security patches; tablets and cellphones should be up to date with approved IOS/Android version levels. Outdated devices that can no longer support an approved software release by providers should not be allowed connection to your organization's network.
- If an employee roots, jailbreaks or modifies the operating system, that device should be removed or blacklisted.
- Work-related data and information should be strictly segregated to support discovery requirements and data retention policies. For the same reason, avoid using personal accounts for work-related emails.
- Enforce device encryption of all storage.
- Mandate that Android/IOS devices have a passcode compliant with your organization's requirements.
- An approved mobile device or application management agent must be used to help control and secure devices such as smartphones and tablets.
- Managed devices should timeout and lock after a set period of inactivity.

As everyone has settled into new routines, please be sure to remind employees that if they are using their personally-owned systems or devices for business purposes, it should be noted that even though they own the devices, they contain bank-owned information; therefore, they may be subject to the same controls that apply to your organization's owned devices.

Keep in mind that it is important that BYOD policies are maintained to protect sensitive customer data and bank information from exposure, as well as safeguarding against the increasing attempts of invasions by malware and ransomware.

Additional loss control resources for your bank are available on **Insights at abais.com**.

ABA Insurance Services | MEMBER OF GREAT AMERICAN INSURANCE GROUP

Visit abais.com for more loss control information or to view this SafeAlert bulletin online. To subscribe to SafeAlert®, request reprints, or if you have questions about this bulletin, please contact ABA Insurance Services at marketing@abais.com or 800-274-5222.